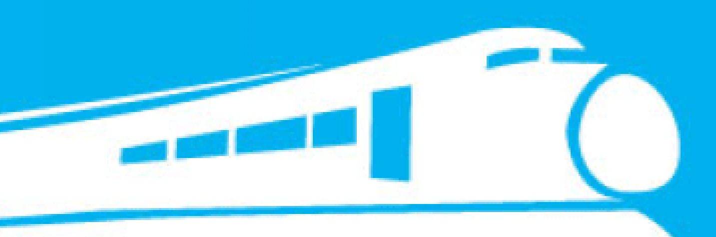
网络工程师

实用培训教程系列

丛书主编　刘晓辉　张运凯　李福亮



计算机网络安全

○王文斌　王黎玲　等编著



清华大学出版社

网络工程师实用培训教程系列
丛书主编：刘晓辉　张运凯　李福亮

计算机网络安全

王文斌　王黎玲　等编著

清华大学出版社
北　京

内 容 简 介

本书主要以现有企业网络为模型，分别介绍服务器系统安全、网络应用服务安全、网络设备安全、网络安全设备管理、局域网接入安全、Internet 接入安全和远程访问安全等内容，全面涵盖了当前主要网络中可能遇到的信息安全问题，并详细介绍了不同的网络安全方案。本书紧密依托选定项目，对企业网络安全中常用的技术进行了深入浅出的讲解，可以帮助读者快速掌握最基本的计算机网络安全技术，打造安全、可靠的企业网络环境。

本书既可作为培养 21 世纪计算机网络安全工程师的学习教材，同时也是从事计算机网络安全的规划、设计、管理和应用集成的专业技术人员的必备工具书。

图书在版编目(CIP)数据

计算机网络安全/王文斌，王黎玲等编著．—北京：清华大学出版社，2010.6
(网络工程师实用培训教程系列)
ISBN 978-7-302-22550-8

Ⅰ．①计…　Ⅱ．①王…　②王…　Ⅲ．①计算机网络—安全技术—技术培训—教材
Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 069736 号

责任编辑：孟毅新
责任校对：袁　芳
责任印制：

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×260　　**印　　张**：30.25　　**字　　数**：729 千字
版　　次：2010 年 6 月第 1 版　　**印　　次**：2010 年 6 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：034323-01

PREFACE 丛书序

近年来,计算机网络在我国已经得到了较快的发展。许多企业、事业单位、行政机关、司法机构和金融系统构建了高速的办公专用网。各种类型的计算机网络高达数十万个,计算机网络已经深入到我们工作、生活和学习的方方面面。

毫无疑问,大量的网络必然需要大量的网络管理人才。初步估计,到目前为止,仅我国每年需要的网络管理人才就达十余万人。随着网络应用的日益深入以及网络所承载的业务量和数据量的不断增长,网络的重要性和安全性也将与日俱增,对网络管理人员的需求也将随之不断地增长。由此可见,网络管理是一个稳定且前途远大的职业。

综观现有的网络技术培养教材,大多将网络技术进行条块分割,按章节、分模块独立讲授,人为地将紧密联系在一起的各种理论和技术分裂开来。这样所带来的问题就是,学生必须将所学的知识和理论全部融会贯通之后,才能初步掌握作为一个网络技术人员所必须具备的一些基本技能,显然这不符合学生的学习规律,也不符合现实的网络管理实际,同时,也是导致许多网络爱好者望而却步的重要原因。

本丛书具有以下特点。

(1) 案例贯穿。本丛书从最常见、最典型的网络应用情境和需求入手,围绕统一的网络环境、统一的网络规划、统一的网络拓扑、统一的资源分配、统一的网络用户和统一的网络需求,提供全面的网络解决方案,以及实用、够用的网络技术,为网络工程师提供宝典级别的现场技术手册。

(2) 项目驱动。本丛书由情境导入需求,以项目进行教学,再由实训实现强化,进而达到培养技能的目的,最终使学生顺利就业。按照网络构建的工作过程系统化课程开发,以真实的网络管理过程为导向规划课程内容,使读者能够真正掌握网络构建与管理的知识和技能,独立完成相关的网络技术项目。

(3) 贴近实战。本丛书突出"先做后学,边做边学"的主旨,通过"练中求学、学中求练、练学结合、边练边学"的教学内容安排,实现"学得会,用得上"的最终目的。由于全书围绕统一的典型网络工程展开,因此,读者能够非常方便地将教学案例移植到真实的网络项目中,学为所用,学以致用。

(4) 内容全面。本丛书涵盖了作为初、中级网络管理员必须掌握的所有理论和技术,以网络管理的实际需求为导向,以培养基本技能为目的,将枯燥的理论融于实际操作中,从而使学生学得会、记得住、用得上。

(5) 兴趣教学。本丛书设计的教学内容按照"案例情景→需求分析→解决方案→技术操作→理论背景"的结构进行组织,有实际案例、有动手操作、有理论分

析，可以激发读者的学习兴趣和学习的主动性，培养读者解决实际问题的能力，提高读者的综合实战水平。

(6) 注重动手。本丛书加大了动手操作的比重，减弱了理论知识的介绍，以适应特定的读者群，体现“做中学”的宗旨。借助大量的网络实验，可以使读者迅速提高技术和技能。

(7) 涵盖认证。本丛书充分考虑到了网络管理员的职业需求及职业资格认证要求，在内容安排和习题设置上与相关认证紧密结合，基本涵盖了国内认证(网络管理员、网络工程师)和国际认证(MCSE、CCNA)所涉及的理论和知识技能，以帮助学生获取“双证书”——学历证书和职业资格证书，增强学生的就业竞争力。

(8) 资深作者。本丛书作者全部来源于网络教学、网络管理和网络工程第一线，具有非常丰富的网络设计、施工和管理经验，既掌握理论技术，又通晓实际操作。作者们做了大量的技术需求和人才需求调研，多次修改提纲以使其更加符合网络搭建和管理实际。

(9) 深度支持。本丛书不仅提供优秀的纸质教材，还为教师提供了电子课件和全方位的技术支持，同时设置有 QQ 群在线答疑、E-mail 离线交流和 BBS 论坛互动平台，并为读者提供网络构建方案和配置技术咨询，形成一个让师生更加方便、更加自主学习的教学环境，有效地提升了教师授课和学生学习的能力。

本丛书删繁就简，围绕一个典型的网络工程展开理论和技术讲解，囊括了网络布线、网络搭建、网络管理、网络服务、网络安全、数据存储等各种组网、管网和用网技术。因此，读者学完本套丛书后，可以直接将其应用至自己的工作实践。即使是初学者，只要熟悉 Windows 的一般操作，就能非常容易地上手，迅速成长为一名合格的网络管理员。

刘晓辉

2010 年 6 月

FOREWORD 前言

随着信息化进程的推进，几乎所有的企事业单位都有自己的网络，而由此产生的网络管理人才的需求缺口正在逐年扩大。据相关部门统计，2009 年网络管理人才缺口达到 13.5 万人，许多企业不惜重金，招募一名出色的网络管理人员。随着网络应用的不断拓展，企业发展对计算机网络的依赖性将越来越强，而掌握大量精尖网络技术的人才也会变得越来越受欢迎。为什么在如此光明的就业形势下，却经常听到网络管理员的工资只有几百元呢？原因很简单，企业真正需要的网络管理员是能够独当一面的专业人员。向网络工程师晋升，是摆在网络管理员面前的唯一出路。

本套丛书作为网络工程师培训教材，以实际的公司网络为案例，以打造实用的网络工程为目标，以实用和技能为主，摒弃了复杂的原理，以简明的操作为引导，通俗易懂，上手容易。读者只需按照书中的操作来学习，就能掌握相应的技能，学完全套书之后，即可掌握大部分的网络知识。

计算机网络技术的应用虽然加速了企业发展的步伐，但随之而来的安全问题，也时刻威胁着企业的根本利益。近年来，企业网站遭到篡改，病毒泛滥成灾，商业机密失窃，企业网络瘫痪，各种高科技信息犯罪活动正在严重危害着社会的发展和企业的生存。本书以中小型企业的计算机网络安全为例，全面、系统地介绍了企业网络的安全建设，旨在帮助企业打造安全、可靠、高效、便捷的计算机网络。

全书内容共分为 13 章，技术操作与需求目标紧密结合，并对应用到的新技术以“知识链接”的方式加以剖析。第 1 章网络安全规划，从整个网络的安全管理任务出发，对整个网络项目的安全需求进行全面分析和规划。第 2 章 Windows 系统安全，以 Windows Server 2008 为例介绍服务器系统安全，包括常规安全配置、系统漏洞安全、管理员账户安全等。第 3 章网络服务安全，介绍常用网络服务的安全，包括活动目录服务、WWW 服务、FTP 服务等的安全配置与管理。第 4 章文件权限管理，介绍 AD RMS、IRM 文件权限保护技术在企业网络中的应用和配置。第 5 章网络病毒防御，以 Symantec 网络防病毒系统为例，介绍局域网防病毒系统的部署与应用。第 6 章系统补丁更新，介绍如何通过 WSUS 服务器实现企业网络中计算机的系统补丁管理。第 7 章 Cisco IOS 安全，介绍常用 Cisco 网络设备基于 IOS 的安全，包括交换机、路由器、无线 AP 的安全配置。第 8 章局域网接入安全认证，介绍如何通过“Cisco ACS + Active Directory”模式实现网络设备接入的 802.1x 身份验证。第 9 章 Internet 接入安全，介绍如何通过 Forefront TMG 实现局域网共享接入、安全防护以及内网服务器的发布。第 10 章远程接入安全，介绍远程接入 VPN 技术在企业网络中的应用，包括 IPSec VPN、SSL VPN 的部署与测

试等。第 11 章网络访问保护，介绍 NAP 技术的部署及应用，包括 IPSec 强制技术、802.1x 强制技术、VPN 强制技术以及 DHCP 强制技术的实施。第 12 章安全设备规划与配置，介绍企业网络中常用安全设备的规划与部署，包括 Cisco ASA、IPS、IDS 等。第 13 章配置网络可靠性，介绍通过故障转移群集和网络负载均衡技术，以及网络设备的链路冗余技术提高企业网络的可靠性。

为了让读者更深入地了解所学的知识，在每章的最后还配备了习题和实验，从而可以起到复习和测验的作用，能使读者尽快迈向网络工程师的行列。

本书可作为大中专院校计算机网络专业的教材，也可作为中小型网络管理员、网络工程技术人员和网络爱好者的参考书。

本丛书由刘晓辉、张运凯、李福亮主编。本书由王文斌、王黎玲等编著。具体分工如下：王文斌编写了第 1～4 章，王黎玲编写了第 5～8 章，李文俊编写了第 9～10 章，王同明编写了第 11 章，石长征编写了第 12 章，郭腾编写了第 13 章。编者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，本书作为对一段工作的总结与回顾，希望能对大家的系统维护和网络管理工作有所帮助。

由于编者水平有限，书中难免有不足之处，恳请广大读者批评指正。

编　者

2010 年 4 月

CONTENTS

目 录

第 1 章 chapter 1

网络安全规划

随着计算机应用的日益普及，网络已经成为大多数企业的重要组成部分，许多常规办公应用已经开始转向网络，例如企业办公、视频会议、合作伙伴沟通等。随之而来的网络安全问题，也就成为制约企业生存与发展的命脉。网络安全建设的总体思路是：以信息资产为核心，以安全战略为指导，根据安全需求逐步完善安全基础设施，为网络应用提供安全能力支持。

1.1 项目背景

某高新产品研发企业拥有员工 2000 余人，公司总部坐落在省会城市高新技术开发区，包括 4 个生产车间和两栋职工宿舍楼，产品展示、技术开发与企业办公均在智能大厦中进行。该企业在外地另开设有两家分公司，由总公司进行统一管理和部署。目前，该企业网络的拓扑结构如图 1-1 所示，基本情况如下。

(1) 公司局域网已经基本覆盖整个厂区，中心机房位于智能大厦的第 3 层(共 15 层)，职工宿舍楼和生产车间均有网络覆盖。

(2) 网络拓扑结构为“星型+树型”，接入层交换机为 Cisco Catalyst 2960，汇聚层交换机为 Cisco Catalyst 3750，核心层交换机为 Cisco Catalyst 6509。

(3) 现有接入用户数量为 500 个，客户端均使用私有 IP 地址，通过防火墙或代理服务器接入 Internet。部分服务器 IP 地址为共有 IP 地址。

(4) Internet 接入区的防火墙主要提供 VPN 接入功能，用于为远程移动用户或子公司网络提供远程安全访问。

(5) 会议室、产品展示大厅等公共场所部署无线接入点，实现随时随地无线漫游接入。

(6) 服务器操作系统平台多为 Windows Server 2003 和 Windows Server 2008 系统。客户端系统为 Windows XP Professional 和 Windows Vista。

(7) 网络中部署有 Web 服务器，为企业网站提供运行平台。

(8) 企业网络办公平台为 WSS，文件服务器可以为智能大厦的办公用户提供文件共享、存储与访问。

(9) E-mail 用于员工之间的彼此交流，以及企业与外界的通信联络。

(10) 打印服务和传真服务主要满足智能大厦用户网络办公的应用。

(11) 企业分支结构通过 VPN 方式远程接入总部局域网，并且可以访问网络中的共享资源。

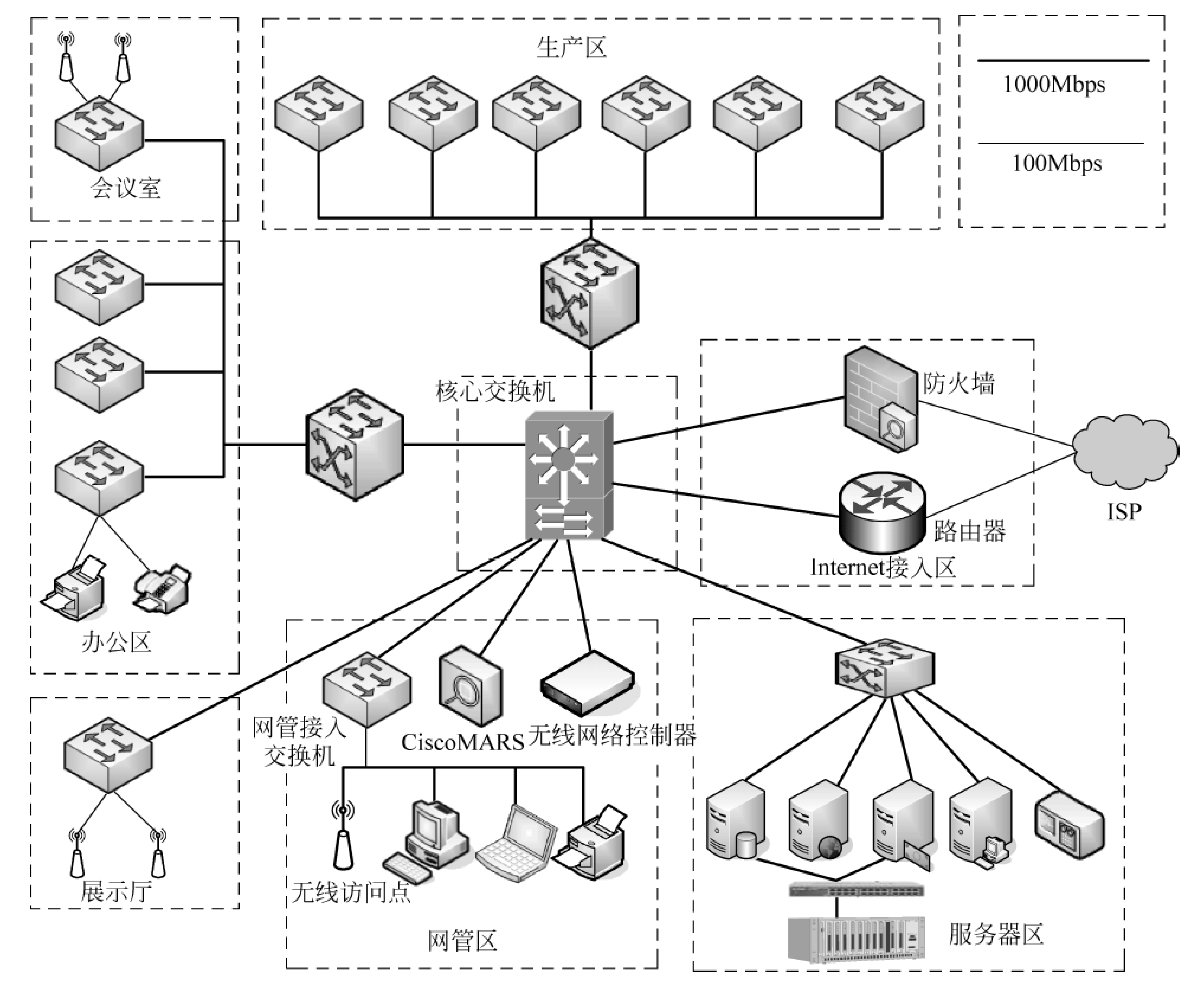


图 1-1 项目背景

1.2 项目分析

在普通小型局域网中，最常用的安全防护手段就是在路由器后部署一道防火墙，甚至安全需求较低的网络并无硬件防火墙，只是在路由器和交换机上进行简单的访问控制与数据包筛选机制就可以了。但是，在该企业网络中，许多重要应用都要依赖网络，势必对网络安全性的要求要高一些，在部署网络安全设备的同时，必须辅助多种访问控制与安全配置措施，加固网络安全。

1.2.1 安全设备分布

1. 防火墙

由于企业局域网采用以太网接入方式，所以直接使用防火墙充当接入设备，部署在网络边缘，防火墙连接的内网路由器上配置访问列表和静态路由信息。另外，在会议室、产品展示厅等公共环境中的汇聚交换机和核心交换机之间部署硬件防火墙，防止公共环境中可能存在的安全风险通过核心设备传播到整个网络。

2. IPS

IPS(Intrusion Prevention System，入侵防御系统)部署在 Internet 接入区的路由器和

核心交换机之间,用于扫描所有来自 Internet 的信息,以便及时发现网络攻击和制定解决方案。

3. IDS

IDS(Intrusion Detection System,入侵检测系统)本身是一个典型的探测设备,类似于网络嗅探器,无须转发任何流量,而只需要在网络上被动地、无声息地收集相应的报文即可。IDS 无法跨越物理网段收集信息,只能收集所在交换机的某个端口上的所有数据信息。该网络中的 IDS 部署在安全需求最高的服务器区,用于实时侦测服务器区交换机转发的所有信息。对收集来的报文,IDS 将提取相应的流量统计特征值,并利用内置的入侵知识库,与这些流量特征进行智能分析比较匹配。根据默认的阈值,匹配耦合度较高的报文流量将被认为是进攻,IDS 将根据相应的配置进行报警或进行有限度的反击。

4. Cisco Security MARS

Cisco Security MARS(Monitoring Analysis and Response System)是基于设备的全方位解决方案,是网络安全管理的关键组成部分。MARS 可以自动识别、管理并抵御安全威胁,它能与现有网络和安全部署协作,自动识别并隔离网络威胁,同时提供准确的清除建议。在本例企业网络中,MARS 直接连接在核心交换机上,用于收集经过核心交换机的所有数据信息,自动生成状态日志,供管理员调阅。

1.2.2 网络设备安全现状

当前网络中的交换机、路由器等网络设备全部都是可网管的智能设备,并且提供 Web 管理方式,同时配置了基本的安全防御措施,如登录密码、用户账户权限等。

1. 交换机和路由器安全配置

交换机的主要功能就是提供网络接入所需的接口。目前,该网络中基于交换机的安全管理仅限于 VLAN 划分、Enable 密码和 Telnet 密码等基本安全措施,并未进行任何高级安全配置,如流量控制、远程监控、IEEE 802.1x 安全认证等,存在较大的安全隐患。

企业网络采用以太网接入 Internet,而网络中部署的网络防火墙已具备接入功能,所以该网络中的路由器上只配置了简单的静态路由、访问控制列表和网络地址转换,可以满足基本的安全需求。

2. 办公设备安全配置

企业网络中的集中办公设备包括打印机和传真机,均支持网络接入功能,部署在楼层的集中办公区。由于缺乏访问权限控制措施,致使网络打印机和传真机被滥用,造成不必要的资源浪费。另外,用户计算机到打印机之间的数据传输是未经加密的明文,存在一定的安全隐患。

1.2.3 服务器部署现状

网络中的应用服务器包括域控制器、DHCP 服务器、文件服务器、打印服务器、传真服务器、网络办公平台、数据库服务器等,其中有多种网络服务合用一台服务器,网络中共有服务器 10 台,通过单独的交换机高速连接至核心交换机,完全采用链路冗余结束双线连接,确保连接的可靠性。

所有服务器均已加入域中,接受域控制器的统一管理,并且已开启远程终端功能,用户

可以使用有效的管理员账户凭据远程登录服务器,实现相应的配置与管理任务。

1.2.4 客户端计算机

客户端计算机主要以 Windows 操作系统为主,极少数用户是运行 Linux 和 Mac OS 操作系统的。客户端计算机的安全防御比较薄弱,仅限于用户账户登录密码、个人防火墙、杀毒软件等。因此,由于个别客户端感染病毒而导致网络瘫痪的问题时有发生。对于 Windows 系统而言,应用最多的 Windows XP Professional 和 Windows Vista 系统已经集成了比较完善的安全防御功能,如 Internet 防火墙、Windows 防火墙、Windows Defender、Windows Update 等,客户端用户只需对这些功能进行简单配置,即可增强系统安全性。

另外,对于中型规模的企业网络而言,统一的网络管理才是最重要的。例如,统一配置客户端计算机安全功能、部署 WSUS 服务器、增强网络访问控制、部署 NAP 系统等。

1.2.5 无线局域网安全现状

在企业网络中部署无线局域网,延伸了有线局域网的覆盖范围,避免网络布线对现有整体布局和装修的破坏,既是环境需求,也是企业发展和生存的需要。用户在无线网络覆盖范围内可以自由访问网络,充分享受无线畅游的便利。但是,由于无线网络传输的特殊性,无线局域网的安全问题也是不容忽视的。该企业网络中的无限网络安全问题,主要表现在如下几个方面。

1. WEP 密钥的发布问题

802.11 本身并未规定密钥如何分发。所有安全性考虑的前提是假定密钥已通过与 802.11 无关的安全渠道送到了工作站点上,而在实际应用中,一般都是手工设置,并长期固定使用 4 个可选密钥之一。因此,当工作站点增多时,手工方法的配置和管理将十分烦琐且效率低下,而且密钥一旦丢失,WLAN 将无安全性可言。

2. WEP 用户身份认证方法的缺陷

802.11 标准规定了两种认证方式:开放系统认证和共享密钥认证。

开放系统认证是默认的认证方法,任何移动站点都可加入 BSS(Basic Service Set,基本服务集),并可以跟 AP(Access Point,接入点)通信,能“听到”所有未加密的数据,可见,这种方法根本没有提供认证,也就不存在安全性。

共享密钥认证是一种请求响应认证机制:AP 在收到工作站点 STA(Static Timing Analysis,静态时序分析)的请求接入消息时发送询问消息,STA 对询问消息使用共享密钥进行加密并送回 AP,AP 解密并校验消息的完整性,若成功,则允许 STA 接入 WLAN。攻击者只需抓住加密前后的询问消息,加以简单的数学运算就可得到共享密钥生成的伪随机密码流,然后伪造合法的响应消息通过 AP 认证后接入 WLAN。

3. SSID 和 MAC 地址过滤

WEP 服务集标识 SSID 由 Lucent 公司提出,用于对封闭网络进行访问控制。只有与 AP 有相同的 SSID 的客户站点才允许访问 WLAN。MAC 地址过滤的想法是 AP 中存有合法客户站点的 MAC 地址列表,拒绝 MAC 地址不在列表中的站点接入被保护的网络。但由于 SSID 和 MAC 地址很容易被窃取,因此安全性较低。

4. WEP 加密机制的天生脆弱性

WEP 加密机制的天生脆弱性是受网络攻击的最主要原因,WEP2 算法作为 802.11i 的安全标准,对现有系统改进相对较小并易于实现。

1.3 项目需求

由于该公司的主要业务为高新产品开发和生产,掌握众多行业机密信息,并且下设多个部门,所以对网络安全性和稳定性要求比较高。无论是基础网络还是客户端都必须严格做好安全防御工作。

1.3.1 网络安全需求

综合项目成本和实际应用等多方面因素,可以从如下几个方面满足用户需求。

(1) 将防火墙部署在网络边缘,用于隔离来自 Internet 的所有网络风险。

(2) 在路由器和核心交换机之间部署 IPS,对全网的所有 Internet 通信进行检测,以便可以自动阻止、调整或隔离非正常网络请求和危险信息的传输。

(3) 生产区和办公区分别通过汇聚交换机连接至核心交换机,在相应的汇聚交换机上分别进行适当的安全配置,将可能存在的风险因素隔离在网络局部。

(4) 在办公区网络中,将安全需求和应用需求不同的用户指定到不同的 VLAN 中,充分确保部门内部和部门间的信息安全。

(5) 在会议室和展示厅等移动用户比较集中的场所,部署无线接入系统,在无线接入点以及无线接入点连接的接入交换机上,分别部署相应的安全防御措施,如 IEEE 802.1x 认证、禁止广播 SSID、WEP 加密等。

(6) 网络管理区和服务器区直接连接至核心交换机,以确保网络传输的可靠性。网络管理区中部署有 MARS 系统,用于监控、分析和处理网络中所有通过核心交换机的数据通信,以便及时发现网络中存在的恶意攻击、非正常访问等情况,并协助管理员制定相应的解决方案。

(7) 为了确保服务器的安全,在服务器集中区部署 IDS,可以对服务器区网络以及系统的运行状况进行监视,尽可能发现各种攻击企图、攻击行为或者攻击结果,以保证网络系统资源的机密性、完整性和可用性。

1.3.2 网络访问安全需求

由于公司大部分用户信息安全意识较差,因此必须对安全需求较高的部门的用户进行集中管理,防止机密信息外泄。另外,本公司在外地设有分公司,只能通过远程接入方式访问内部网络资源,可以借助 VPN 技术实现加密传输,充分确保信息安全。目前,该网络中网络访问安全需求如下。

(1) 客户端更新需要集中管理。大多数用户都已启用 Windows Update 功能,但是每个用户都从微软官方站点下载更新程序,会占用大量的网络带宽。另外,还有部分用户并未开启 Windows Update 功能,存在可能招致网络攻击的安全漏洞。

(2) 网络病毒不得不防。网络病毒和攻击是目前最主要的信息安全威胁因素。网络病

毒的防御工作绝非一蹴而就,必须从各方面严格防范。通常情况下,大部分用户都安装了杀毒软件和个人防火墙软件,可以起到一定的安全防护作用,但是未能升级病毒库同样可能感染病毒。更严重的是,部分用户不安装任何杀毒软件和防火墙就开始使用,这是非常危险的。

(3) 网络访问控制需求。网络中缺乏严格的访问控制措施,用户只需使用相应的用户账户和密码即可接入网络和访问共享资源,而对客户端系统健康程度没有任何要求和限制。如果接入用户的计算机已经感染病毒,则病毒可能通过网络快速蔓延至整个网络的所有分支。

(4) 远程访问安全的保护。远程接入是该网络中的重要应用之一,用于实现分公司网络到总公司网络的互联。远程访问 VPN 技术本身就具有一定的安全性,同时采用隧道和加密等多种技术,但是为了确保远程访问的安全,应加强远程访问的保护与控制。

1.4 项目规划

网络安全与网络应用是相互制约和影响的。网络应用需要安全措施的保护,但是如果安全措施过于严格,就会影响到应用的易用性。因此,部署网络安全措施之前,必须经过严格的规划。另外,网络安全的管理遍布网络的所有分支,包括设备安全、访问安全、服务器安全、客户端安全等。

1.4.1 服务器安全规划

服务器是企业网络的重要基础,其安全性将直接影响企业网站以及网络应用的安全,甚至会影响企业的生存与发展。服务器的大部分应用都是基于网络操作系统等软件实现的,因此,无论是应用程序出错,还是硬件故障都可能导致服务器瘫痪。若想做好服务器安全防护工作,必须从多方面入手。

1. 服务器硬件安全

服务器硬件设备的维护主要包括增加和卸载设备、更换设备、工作环境维护等。因为服务器的运行是不间断的,因此这些维护工作必须在确保服务器正常运行的状态下进行。

(1) 增加内存和硬盘容量。服务器的内存和硬盘都是支持热插拔的,建议增加与原设备同厂商、同型号、同容量的内存或硬盘,避免由于兼容性问题而导致服务器宕机。

(2) 定期为服务器除尘。很多服务器故障都是由于内部灰尘导致的,因此建议管理员每个月定期拆机打扫一次。

(3) 控制机房温度和湿度。虽然服务器对工作环境的要求比较宽泛,但是当服务器周边环境比较恶劣时同样会降低其处理速度和稳定性。

2. 操作系统安全

服务器操作系统的安全是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。对于操作系统的安全防范可以采取如下策略。

(1) 对操作系统进行安全配置,提高系统的安全性。系统内部调用不对 Internet 公开,关键性信息不直接公开,尽可能采用安全性高的操作系统。

(2) 应用系统在开发时,采用规范化的开发过程,尽可能地减少应用系统的漏洞。

(3) 网络上的服务器和网络设备尽可能不采取同一家的产品。

(4) 通过专业的安全工具(安全检测系统)定期对网络进行安全评估。

3. 网络应用服务安全

局域网中常用的网络服务包括 WWW 服务、FTP 服务、DNS 服务、DHCP 服务、Active Directory 服务等，随着服务器提供的服务越来越多，系统也容易混乱、安全性也将降低，因此，就需要对网络服务的相关参数进行设置，以增强其安全性和稳定性。通常情况下，网络应用服务安全可以分为如下 4 层。

(1) 网络与应用平台安全：主要包括网络的可靠性与生存性、信息系统的可靠性和可用性。网络的可靠性与生存性依靠环境安全、物理安全、节点安全、链路安全、拓扑安全、系统安全等方面来保障。信息系统的可靠性和可用性主要由计算机系统安全性决定。

(2) 应用服务提供安全：主要包括应用服务的可用性与可控性。服务可控性依靠服务接入安全以及服务防否认、服务防攻击、国家对应用服务的管制等方面来保障。服务可用性与承载业务网络可靠性以及维护能力等相关。

(3) 信息存储与传输安全：主要包括信息在网络传输和信息系统存储时完整性、机密性和不可否认性。信息完整性可以依靠报文鉴别机制；信息机密性可以依靠加密机制以及密钥分发等来保障；信息不可否认性可以依靠数字签名等技术来保障。

(4) 信息内容安全：主要指通过网络应用服务所传递的信息内容不涉及危害国家安全，泄露国家机密或商业秘密，侵犯国家利益、公共利益或公民合法权益，从事违法犯罪活动。

1.4.2　客户端安全规划

目前，Windows XP 和 Windows Vista 是首选客户端操作系统，为了便于统一管理，应将相对固定的客户端计算机加入域，接受域控制器的统一管理。通常情况下，可以从如下 5 方面做好客户端计算机的安全防御工作。

(1) 对于加入域的计算机可以通过组策略等工具统一部署安全策略，例如用户账户策略、密码策略、硬件设备安装限制策略等，确保客户端的安全。

(2) 对于未加入域的计算机，应提高用户网络安全的意识，通过设置登录密码、计算机锁定、防火墙等方式，确保系统安全。

(3) 在网络中部署 WSUS 服务器，负责为所有客户端计算机和服务器提供系统更新，避免系统漏洞的产生。

(4) 在所有客户端上部署 Symantec 网络防病毒客户端软件，并接受服务器端的统一管理，开启自动更新病毒库功能。

(5) 灵活部署和运用 Windows 防火墙、Windows Defender 等系统集成安全防护程序。

1.4.3　网络设备安全规划

局域网中的主要网络设备包括路由器、交换机和防火墙，分别用于提供不同的网络功能和应用。网络设备的部署方式、工作环境、配置管理等，都可能影响其安全性。

1. 网络设备的脆弱性

通常情况下，当用户按照组网规划方案购入并部署好网络设备之后，设备中的主要组成

系统即可在一段时间内保持相对稳定地运行。但是,网络设备本身就有一定的脆弱性,这也往往会成为入侵者攻击的目标。网络设备的安全脆弱性主要表现在如下5方面。

(1) 提供不必要的网络服务,提高了攻击者的攻击机会。

(2) 存在不安全的配置,带来不必要的安全隐患。

(3) 不适当的访问控制。

(4) 存在系统软件上的安全漏洞。

(5) 物理上没有得到安全存放,容易遭受临近攻击。

针对这些与生俱来的安全弱点,用户可以通过如下措施加固设备安全。

(1) 禁用不必要的网络服务。

(2) 修改不安全的配置。

(3) 利用最小特权原则严格对设备的访问控制。

(4) 及时对系统进行软件升级。

(5) 提供符合 IPP(Information Protection Policy,信息保护策略)要求的物理保护环境。

2. 部署网络安全设备

局域网中常见的网络安全设备包括网络防火墙、入侵检测设备、入侵防御设备等。网络防火墙是必不可少的,用于拦截处理来自 Internet 的各种攻击行为,并且可以隔离内部网络有效避免内部攻击。入侵检测设备只能用于记录入侵行为,局域网中已经很少使用。通常情况下,可以在网络中部署入侵防御系统,保护内部服务器或局域网的安全。

3. IOS 安全

IOS 就是智能网络设备的网络操作系统,主要用于提供软件管理平台。IOS 与计算机操作系统类似,难免存在系统漏洞,入侵者同样可以通过这些漏洞进入网络设备的 IOS,进行各种破坏活动,从而影响网络的正常运行。

通常情况下,用户可以从如下6方面实现网络设备的 IOS 安全。

(1) 配置登录密码,主要包括 Enable 密码和 Telnet 密码,必要时可以以加密方式存储密码,以确保其安全性。

(2) 配置用户访问安全级别,为不同的管理账户赋予不同的访问和管理权限。

(3) 控制终端访问安全,严格控制允许终端连接的数量,以及终端会话超时限制。

(4) 配置 SNMP 安全。SNMP 字符串用于验证用户与交换机的连接,确保其身份的有效性,类似于用户账户和密码。

(5) 及时备份 IOS 映像,以便出现误操作或遭遇攻击时可以迅速恢复。

(6) 升级 IOS 版本。IOS 的系统漏洞是不可避免的,用户可以通过安装补丁或升级 IOS 版本的方法避免由于系统漏洞导致的网络攻击。

1.4.4 无线设备安全规划

无线接入不仅是企业发展的需要,更是企业形象的代表。无线局域网是有线网络的扩展,主要用于为移动终端用户提供网络接入。该公司中的 AP(Access Point,无线接入点)主要分布在产品展示区和会议室,方便移动用户随时随地访问公司网络。如今许多笔记本电脑、掌上电脑、手机等都提供无线接入功能,在无线网络覆盖范围内“蹭网”已经成为一种

时尚，对于管理员而言，无线网络安全自然也就成了管理重点。

在无线局域网管理中，可以采用如下措施确保网络安全。

(1) 确保桌面计算机和服务器系统实现尽可能的安全。这种保护提高了攻击的门槛，即使攻击者进入了 WLAN，仍然很难渗透进用户的计算机。

(2) 启用无线 AP 和工作站所支持的最强 WEP。同时，确保拥有一个强健的 WEP 密码，这个密码应该符合有线网络中所应用的相同的密码强度规则。

(3) 确保无线网络的网络名称(SSID)不是可以轻松识别的。不要使用公司名称、自己的姓名或者地址作为 SSID。

(4) 如果无线 AP 支持 SSID 广播，应当关闭。这个措施可以创建一个封闭网络，这样，新的客户端必须在连接之前输入正确的 SSID。

(5) 使用 IEEE 802.1x 身份验证协议保护无线网络的安全。

(6) 在网络中部署无线网络控制器，统一管理和部署网络中的所有无线接入点，实时监测无线网络攻击情况。

1.4.5 安全设备规划

在安全性需求较高的网络中，网络安全设备是必不可少的。该公司网络中使用的安全设备包括网络防火墙、IDS 和 IPS。

1. 网络防火墙

防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即采用不同安全策略的两个网络连接处，如用户和 Internet 之间、同一企业内部同部门的网络之间等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过设定一定的筛选机制来决定允许或拒绝数据包通过，实现对进入网络内部的服务和访问的审计与控制。网络防火墙是内、外网络数据传输的必经之路。

2. IDS

IDS 是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。入侵检测技术是为保证计算机系统的安全，而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术。IDS 通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。该网络中的 IDS 部署在服务器区的接入交换机处。

IDS 能够检测到的攻击类型通常包括：系统扫描(System Scanning)、拒绝服务(Deny of Service)和系统渗透(System Penetration)。IDS 对攻击的检测方法主要包括：被动、非在线地发现和实时、在线地发现计算机网络中的攻击者。IDS 的主要优势是监听网络流量，但又不会影响网络的性能。作为对防火墙的有益补充，IDS 能够帮助网络系统快速发现网络攻击的发生，可扩展系统管理员的安全管理能力，包括安全审计、监视、进攻识别和响应等，从而提高了信息安全基础结构的完整性，被认为是继防火墙之后的第二道安全闸门。

3. IPS

网络中的 IPS 主要用于拦截和处理传统网络防火墙无法解决的网络攻击，部署在网络中的 Internet 接入区。

传统的防火墙旨在拒绝那些明显可疑的网络流量，但仍然允许某些流量通过，因此，防

火墙对于很多入侵攻击仍然无计可施,而绝大多数 IDS 系统都是被动的,不是主动的,即在攻击实际发生前,往往无法预先发出警报。而入侵防御系统 IPS 则倾向于提供主动防御,其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截,避免其造成损失,而不是简单地在恶意流量传送时或传送后才发出警报。

IPS 是通过直接嵌入到网络流量中实现这一功能的,即通过一个网络端口接收来自外部系统的流量,经过检查确认其中不包含异常活动或可疑内容后,再通过另外一个端口将其传送到内部系统中。此时,有问题的数据包,以及所有来自同一数据流的后续数据包,都能在 IPS 设备中被清除掉。

1.4.6 局域网接入安全规划

根据拓扑结构,可以将局域网分为核心层、汇聚层和接入层 3 个层次。接入层是最终面向用户的,是局域网用户进入网络的接入点,在该层应用保障安全的策略,能为局域网的安全运行提供保障。

1. 常规接入安全措施

在传统有线网络中,通常可以采用 802.1x 认证确保局域网接入的安全,但需要交换机支持和后台的 RADIUS 服务器,同时必须采用国内某些网络厂商提供的 802.1x 解决方案,可以实现用户名、IP 地址、MAC 地址、端口、VLAN、交换机 IP 等的绑定,从而有效避免网络设备、用户等的非法接入。除此之外,防火墙类的产品也可以控制局域网接入,但需要额外投资,并且可靠性不是很高。

在无线局域网中,管理员可以通过如下措施确保接入安全。

(1) 设置 SSID。SSID 是无线局域网的网络名称,通常用于区分不同的网络。无线设备或用户接入网络之前必须提供匹配的 SSID,否则无法接入。SSID 类似于一个简单的口令,阻止非法用户的接入,保障无线局域网的安全。另外,还需要禁止无线设备的 SSID 广播功能。

(2) 配置 MAC 地址访问控制列表。每个网络设备或计算机的网卡都有一个唯一的 MAC 地址,因此通过配置 MAC 地址访问控制列表,可以确保只有经过注册的设备才可以接入网络,阻止未经授权的无线用户接入。

(3) 配置 WEP 加密。WEP 加密主要是针对无线网络中传输的数据而言的,可以用于保护链路层数据的安全。WEP 使用 40 位密钥,采用 RSA 开发的 RC4 对称加密算法,在链路层加密数据。

(4) 配置 802.1x 认证。当无线设备或用户接入无线局域网之前,可以通过 802.1x 认证决定是否允许其继续访问。如果认证通过,则 AP 为无线工作站打开这个逻辑端口,否则不允许接入。

2. NAP 技术

NAP(Network Access Protection,网络访问保护)是 Microsoft 在 Windows Vista 和 Windows Server 2008 提供的全新系统组件,它可以在访问私有网络时提供系统平台健康校验。NAP 平台提供了一套完整性校验的方法来判断接入网络的客户端的健康状态,对不符合健康策略需求的客户端限制其网络访问权限。

为了校验访问网络的主机的健康状况,网络架构需要提供如下功能性领域。

(1) 健康策略验证：判断计算机是否适应健康策略需求。

(2) 网络访问限制：限制不适应策略的计算机访问。

(3) 自动补救：为不适应策略的计算机提供必要的升级，使其适应健康策略。

(4) 动态适应：自动升级适应策略的计算机以使其可以跟上健康策略的更新。

1.4.7 Internet 接入安全规划

企业局域网采用共享方式接入 Internet，并将硬件防火墙 Cisco 5540 部署在局域网边缘。为了便于统一管理客户端 Internet 接入安全，在硬件防火墙的后面部署了 Forefront TMG 服务器，可以提供如下功能。

(1) 网络防火墙。TMG 服务器提供了灵活的防火墙策略配置，允许管理员根据实际需要定制 Internet 访问规则，例如限制特定用户访问 Internet、禁止浏览视频网站等。

(2) Web 访问缓存。TMG 服务器既是网络防火墙，又可以作为 Web 访问代理服务器。管理员可以在 TMG 服务器上开辟专用于存储客户端请求的 Internet 数据的空间，暂时缓存常用数据。当客户端需要再次访问这些 Internet 数据时，在局域网中即可完成，提高了客户端的访问效率。

(3) 安全 VPN 接入功能。通过 TMG 服务器创建 VPN 连接，能够很轻松地建立起各种情况下的 VPN 连接。当本地计算机要和远程计算机通过 TMG 服务器进行通信时，数据封装好后，将通过 VPN 进行收发，充分确保通信过程的安全。

1.4.8 远程接入安全规划

目前，最常用的远程访问方式就是 VPN，主流的安全技术包括 SSL VPN 和 IPSec VPN。SSL VPN 应用比较简单，用户无须进行配置，基于 Web 页面即可实现。IPSec VPN 技术应用比较广泛，不再局限于 Web 方式，同时由于其安装和配置过程比较复杂，应用难度也较大。

1. IPSec VPN 远程安全接入

IPSec 提供了多种安全特性，如数据加密、设备验证、数据完整性、地址隐藏和安全机构(SA)密钥老化等功能。IPSec 标准提供数据完整性或数据加密两种功能。数据完整性分两类：128 位强度 Message Digests(MD-5)-HMAC 和 160 位强度安全散列算法(SHA)-HMAC。由于 SHA 的强度更大，所以更加安全。

2. SSL VPN 远程安全接入

SSL VPN 是工作在应用层和 TCP 层之间的远程接入技术。通常 SSL VPN 的实现方式是在企业的防火墙后面放置一个 SSL 代理服务器。如果用户希望安全地连接到公司网络上，那么当用户在浏览器上输入一个 URL 后，连接将被 SSL 代理服务器取得，并验证该用户的身份，然后 SSL 代理服务器将连接映射到不同的应用服务器上。

1.4.9 网络可靠性规划

对于企业网络而言，许多金融、贸易、电子商务等活动都是通过网络完成的，这就要求企业网络具备很高的可靠性。提高网络可靠性的方法有很多，最常用的就是冗余和容错。

在硬件设备方面，可以通过配置交换机生成树、链路汇聚和链路冗余技术来提高局域网

线路连接的可靠性。其中生成树协议可以帮助管理员快速检查网络连接。当主链路发生故障时，便可以自动接通备份链路，确保网络正常工作。链路汇聚技术可以将多条链路聚合为一组干路，还可以提高网络带宽，更重要的是，链路汇聚可以实现负载均衡，从而大大提高了网络的可靠性。局域网接入区域的路由器虽然仅提供路由选择功能，但其重要性也是不容忽视的。可以通过配置路由冗余充分保证 Internet 连接的可靠性。

在软件方面则可以通过服务器群集技术和网络负载均衡技术，来提高重要服务器的可靠性。除此之外，常规的数据备份也是必不可少的，包括服务角色状态信息备份、服务器系统备份、数据库备份、网络设备配置备份等。

第 2 章 chapter 2

Windows系统安全

计算机系统安全是网络信息安全的基础。目前，Windows 操作系统是应用最多的计算机操作系统之一，市场占有量始终维持在 90%左右。常用的服务器操作系统包括 Windows Server 2003 和 Windows Server 2008；常用的客户端 PC 操作系统包括 Windows XP/Vista/7 等。在局域网中，客户端 PC 的安全配置都是通过服务器端的统一部署实现的。Windows Server 2008 是 Microsoft 公司的扛鼎之作，实用性和安全性都有了很大提高。

2.1 Windows 系统安全规划

任何安全措施都无法确保万无一失，强有力的安全措施可以增加入侵难度，从一定程度上提升系统安全性。通常情况下，用户安装操作系统后，只是进行简单的安全设置，便投入应用，其实这是非常危险的。要想使服务器在复杂的网络环境中平稳运行，必须从各方面实施安全加固。

2.1.1 案例情景

该项目网络中涉及的服务器比较多，主要包括域控制器、Web 服务器、邮件服务器、防病毒服务器和文件服务器等，全部采用 Windows Server 2008 操作系统。Windows 操作系统最大的优点就是简便易用、功能强大，但安全性确是让大多数用户忧心忡忡的问题。通常情况下，用户安全意识较差，甚至连网络服务器都没有任何安全防护措施，这是非常危险的。现在绝大多数计算机病毒都是通过网络传播的，如果网络中的某台计算机系统存在安全漏洞，则很可能会招致网络病毒入侵，并快速蔓延到网络中的其他计算机，严重的情况下可能会导致整个网络瘫痪。因此，必须确保网络中每一台服务器的系统安全。

2.1.2 项目需求

操作系统是实现一切网络服务的基础，因此，首先必须确保 Windows 操作系统的安全，再去考虑网络应用和网络服务的安全。相对于早期版本的 Windows Server 操作系统而言，Windows Server 2008 系统的安全性已经有了很大的提升，系统默认集成了防火墙、用户账户控制、安全组策略等多种安全功能。为了适应大多数用户的配置需求，默认情况下，Windows Server 2008 并未启用所有的安全功能，用户必须根据安全需求一一配置并启用这些功能，充分发挥 Windows Server 2008 系统的安全特性。

2.1.3 解决方案

本章主要介绍如何配置 Windows Server 2008 系统安全，以及借助漏洞扫描工具发现和弥补系统安全漏洞。

1. 安全配置向导

SCW 可以帮助管理员快速完成创建、编辑、应用和回滚安全策略操作。用户可以根据需要创建针对某个服务器角色的安全策略，并且可以将其应用到其他服务器上。

2. 配置 Windows 系统安全功能

常用 Windows 系统的基本安全配置包括 Internet 防火墙、Windows Update、用户账户安全、默认共享安全、组策略安全等内容。Windows Server 2008 和 Windows Vista 系统中还新增了用户账户控制、驱动器加密等安全功能。

3. 系统漏洞扫描

Windows 系统的系统漏洞是在所难免的，如果管理员能够及时发现漏洞并安装相应的补丁程序弥补漏洞，仍可以确保操作系统的安全。MBSA 是 Microsoft 公司推出的产品漏洞扫描工具，不仅可以扫描本地系统漏洞安全，而且可以通过网络扫描远程计算机上运行的 Microsoft 产品存在的漏洞。

4. 端口安全

所谓端口安全就是指使用端口查看工具(netstat 命令)，查看当前系统哪些端口是开放的，其对应的宿主程序是哪些，是否存在安全漏洞。

2.2 安全配置向导

使用 SCW 可以针对已安装的服务器角色创建安全策略，并且导出之后，还可以应用到其他有类似安全需求的服务器上。使用安全配置向导创建的安全策略，可直接应用于所有运行 Windows Server 2008 或者 Windows Server 2003 SP1/SP2/R2 操作系统的网络服务器。本节中以创建 Web 服务安全策略为例进行介绍。

2.2.1 配置安全服务

配置安全服务的具体步骤如下。

(1) 依次选择“开始”→“管理工具”→“安全配置向导”选项，启动“安全配置向导”。用户也可以在“开始”菜单的“开始搜索”文本框中，输入 scw 命令并按 Enter 键来启动安全配置向导。单击“下一步”按钮，显示如图 2-1 所示的“配置操作”对话框。安全配置向导提供了 4 种配置操作。

① 新建安全策略：可以创建用于配置服务、Windows 防火墙、Internet 协议安全(IPSec)设置、审核策略和特定注册表设置的安全策略。安全策略文件是 XML 格式文件，默认保存路径为%systemroot%\security\msscw\Policies。

② 编辑现有安全策略：可以编辑已使用 SCW 创建的安全策略。必须先选择“编辑现有安全策略”，才能浏览到要编辑的安全策略文件所在的文件夹。编辑的策略可存储在本地文件夹或网络共享文件夹中。

③ 应用现有安全策略：使用 SCW 创建安全策略后，可将其应用到测试服务器，或者应用到生产环境。

提示：在将新创建或新修改的安全策略应用到生产环境之前，首先进行测试，然后将安全策略部署到业务系统中，测试可使新策略在生产环境中导致意外结果的可能性降至最低。

④ 回滚上一次应用的安全策略：如果使用 SCW 应用的安全策略使服务器功能达不到预期的效果，或者导致其他非预期结果，则可以回滚该安全策略，将自动从该服务器删除对应的安全策略。

注意：如果策略是在“本地安全策略”中编辑的，在应用策略后，这些更改就不能回滚到应用前的状态。对于服务和注册表值，回滚过程还原了在配置过程中更改的设置。对于 Windows 防火墙和 IPSec，回滚过程取消当前使用的任何 SCW 策略的分配，并重新分配在配置时使用的前策略。

如果是第一次使用安全配置向导，则应选中“新建安全策略”单选按钮。

（2）单击“下一步”按钮，显示如图 2-2 所示的“选择服务器”对话框。在“服务器”文本框中，输入需要进行安全配置的 Windows Server 2008 服务器的主机名或 IP 地址。也可以单击“浏览”按钮，选择需要进行安全配置的目标计算机。

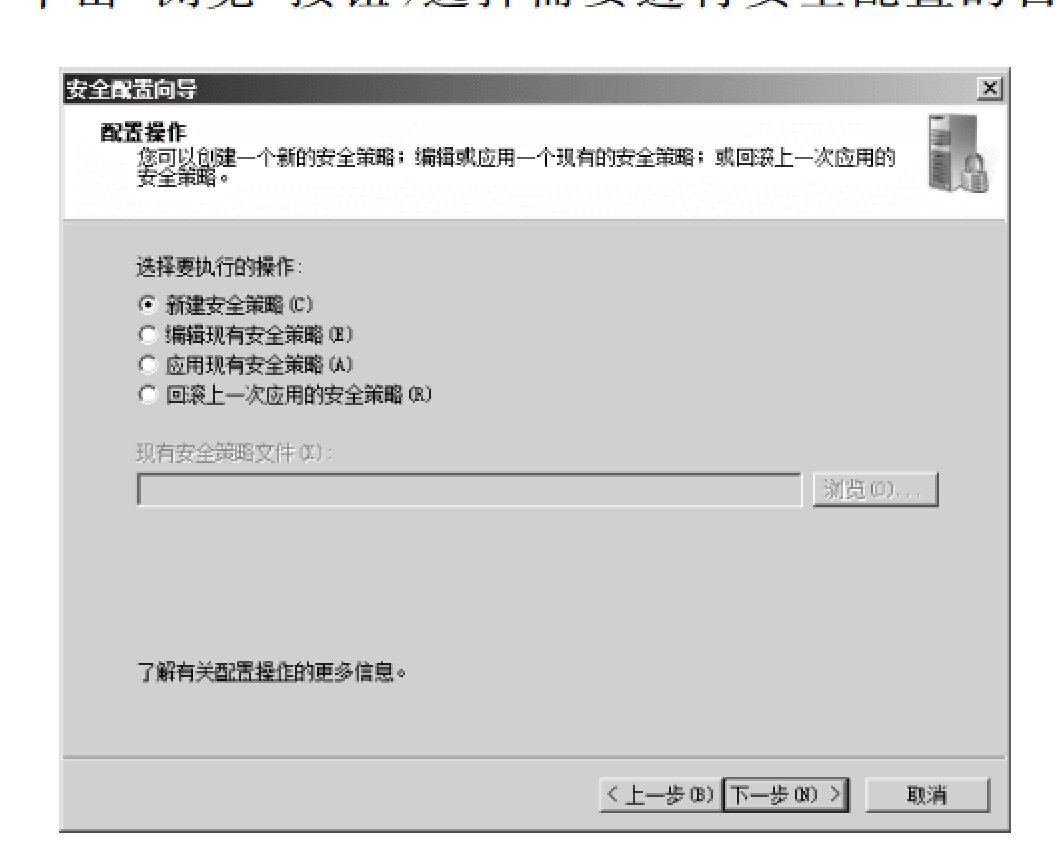


图 2-1　“配置操作”对话框

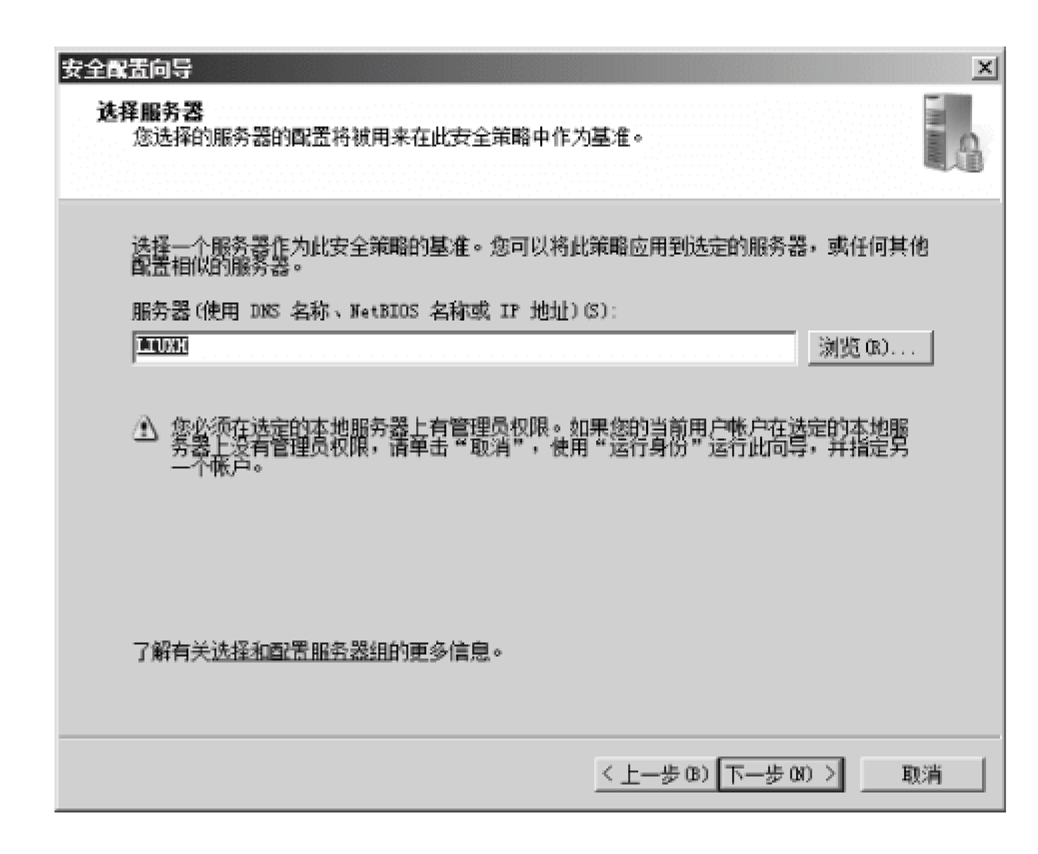


图 2-2　“选择服务器”对话框

（3）单击“下一步”按钮，开始扫描配置数据库，主要包括已安装或运行的网络服务、IP 地址及子网信息等。扫描完成后显示“正在处理安全配置数据库”对话框。单击“查看配置数据库”按钮，可以查看详细扫描结果。需要注意的是，在此过程中由于 Internet Explorer 7.0 的安全设置，可能会出现安全提示信息。单击“下一步”按钮，显示“基于角色的服务配置”对话框，如图 2-3 所示。

（4）单击“下一步”按钮，显示“选择服务器角色”对话框。在“查看”下拉列表框中，系统默认选择“安装的角色”选项，即只设置已安装服务的安全策略，并在“为选定的服务器选择要执行的服务器角色”列表中，选中“Web 服务器”复选框。单击“下一步”按钮，显示“选择客户端功能”对话框。尽管本节主要配置 Web 服务器安全，但服务器本身可能同时又是客户机，如自动更新客户端、DHCP 客户端等，因此还必须保留必要的客户端功能。建议使用默认设置即可，如图 2-4 所示。

（5）单击“下一步”按钮，显示“选择管理和其他选项”对话框。在“查看”下拉列表框中



图 2-3 “基于角色的服务配置”对话框



图 2-4 选择服务器角色和客户端功能

选择“Web 服务器”选项，并在“选择用来管理选定的服务器的选项”列表中，选中“Web 服务器(IIS)的远程管理”复选框。单击“下一步”按钮，显示“选择其他服务”对话框。其他服务是指当前服务器上已经安装但在安全配置数据库中未显示的服务。如果出现这种情况，安全配置向导将在“选择其他服务”对话框中显示已安装的服务列表。展开相应的服务即可查看其详细运行模式，如图 2-5 所示。建议取消无关紧要的其他服务。

(6) 单击“下一步”按钮，显示如图 2-6 所示的“处理未指定的服务”对话框。“未指定的服务”是指安全策略配置向导扫描过程中未能发现的服务，用户可以在这里设置其运行状态，选中“禁用此服务”单选按钮即可。

(7) 单击“下一步”按钮，显示如图 2-7 所示的“确认服务更改”对话框，在列表中显示了当前策略设置的系统服务启动模式的更改。

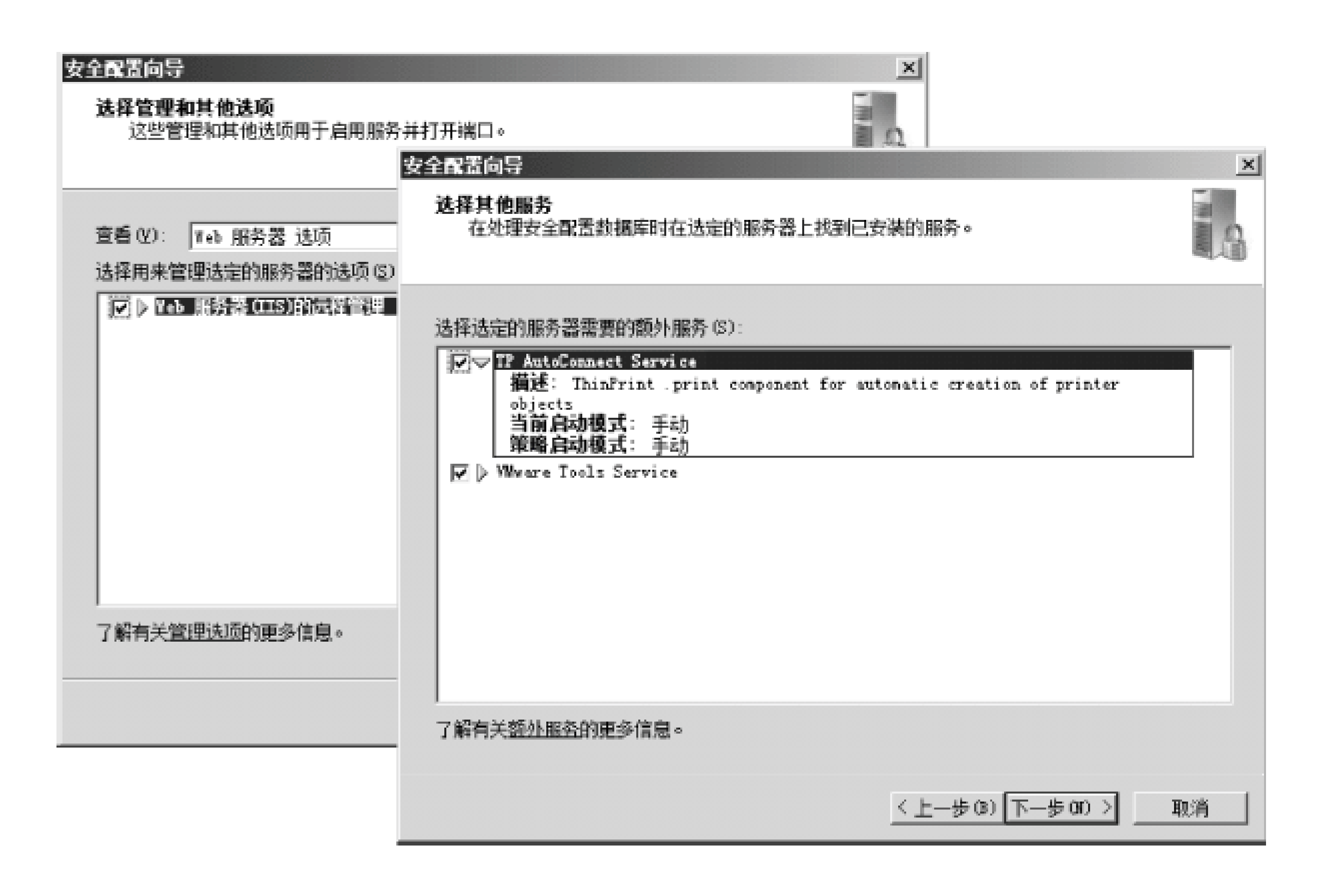
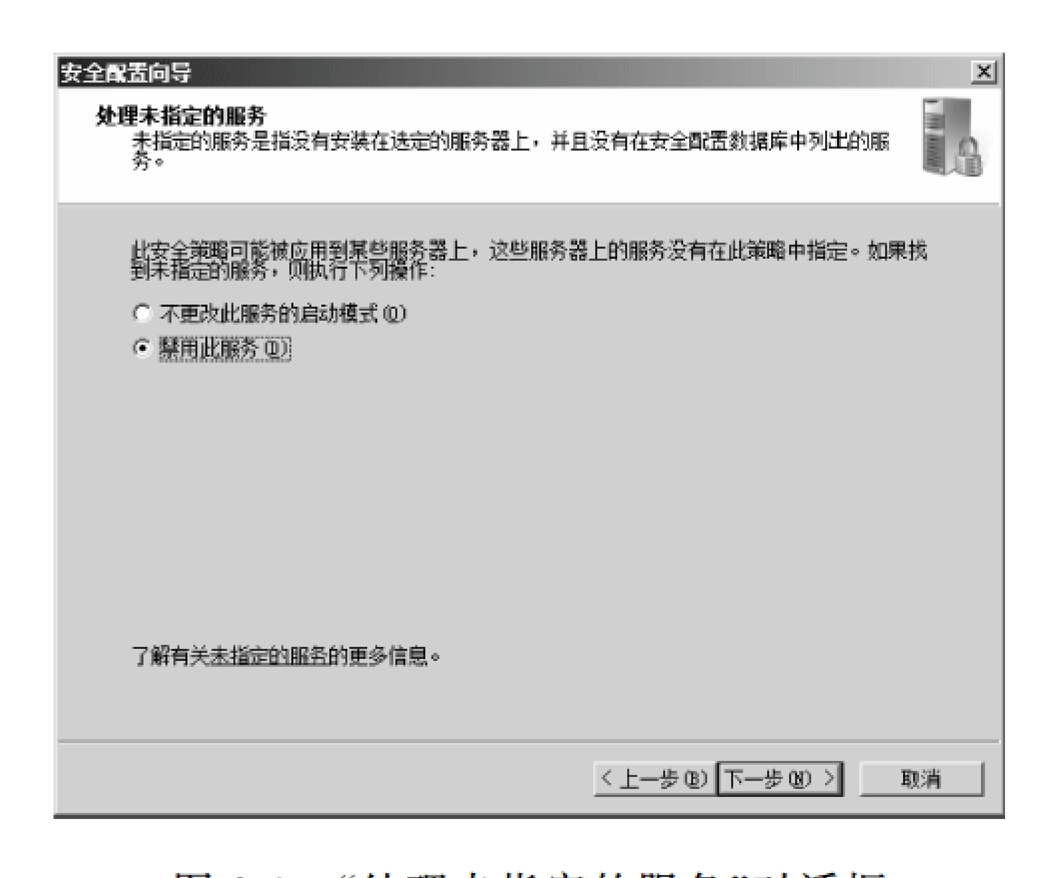


图 2-5　查看已安装服务的详情



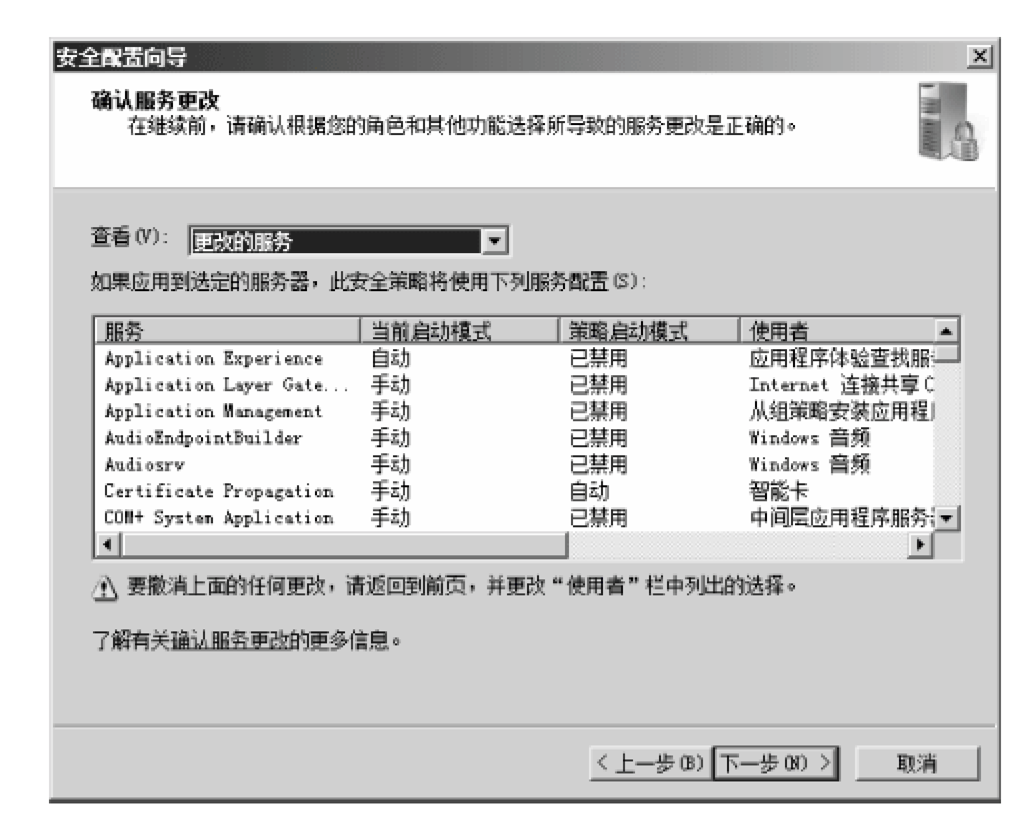




图 2-6　“处理未指定的服务”对话框　　　　图 2-7　“确认服务更改”对话框

（8）单击“下一步”按钮，显示“网络安全”对话框。如果选中“跳过这一部分”复选框，则将跳过“网络安全”配置部分。建议不要跳过此步骤，继续按照如下步骤操作。单击“下一步”按钮，显示“网络安全规则”对话框，在“查看”下拉列表框中选择“选定角色中的规则”选项，如图 2-8 所示。

提示： 如果列表中没有列出需要使用的 Windows 防火墙规则，可以单击“添加”按钮，打开如图 2-9 所示的“添加规则”对话框，将其添加到列表中。在“名称”文本框中，输入防火墙规则的名称，如 www，为了便于区分还可以输入相关的描述信息；在“方向”选项区域中，选中“入站”单选按钮；另外，还可以根据需要在“操作”选项区域中选择相应限制连接方式。

（9）单击“下一步”按钮，显示“注册表设置”对话框。通过该设置可以修改 Windows Server 2008 服务器注册表中一些特殊键值，从而严格限制用户的访问权限。建议用户不要跳过此步骤。单击“下一步”按钮，显示“要求 SMB 安全签名”对话框。设置选定的服务器和客户端的通信信息，保持系统默认的全部选择状态即可，如图 2-10 所示。

（10）单击“下一步”按钮，显示如图 2-11 所示的“出站身份验证方法”对话框。选择当前服务器远程连接到其他计算机时使用的身份验证方法，如果是在域网络中进行远程登录，



图 2-8 “网络安全规则”对话框



图 2-9 “添加规则”对话框



图 2-10 “注册表设置”对话框

则选中“域账户”复选框即可；如果是工作组环境，建议选中“远程计算机上的本地账户”复选框。

(11) 单击“下一步”按钮，显示如图 2-12 所示的“出站身份验证使用本地账户”对话框，此对话框中的选项与所选择的出站身份验证方法有关，这里以使用“远程计算机上的本地账户”验证方法为例。通常情况下，保持默认设置即可。

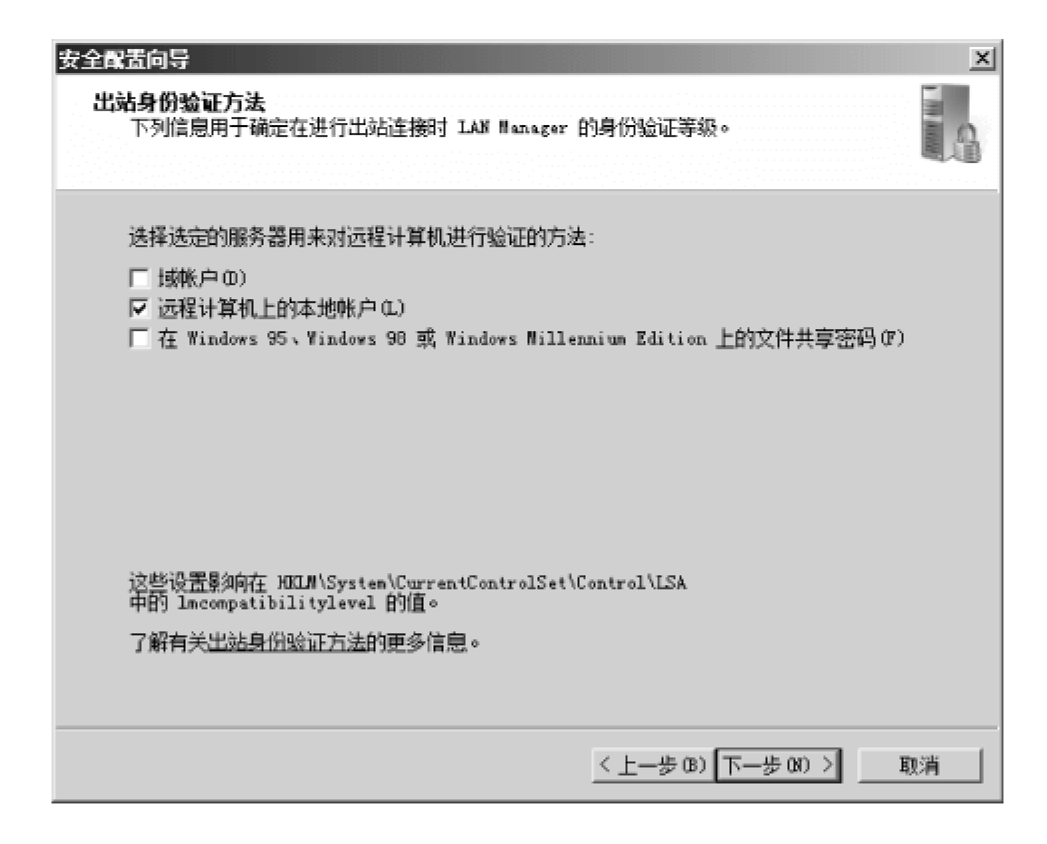



图 2-11　“出站身份验证方法”对话框

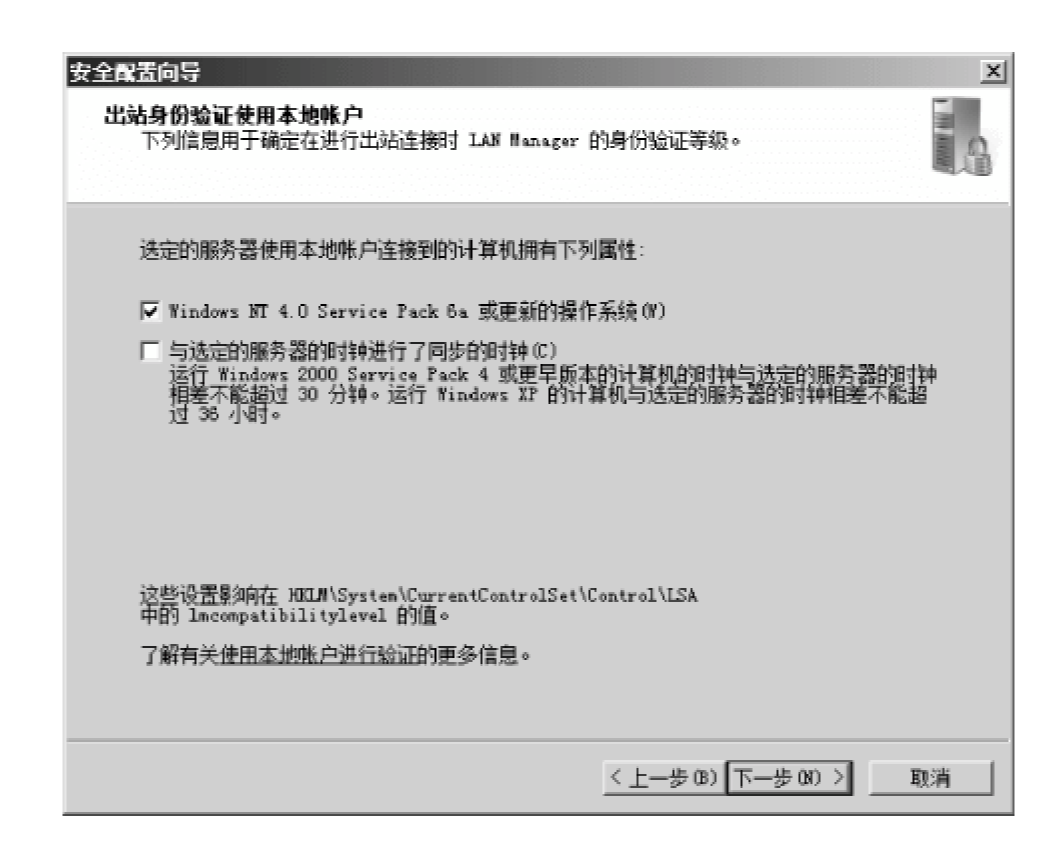


图 2-12　“出站身份验证使用本地账户”对话框

提示：如果不选择任何出站身份验证方法，则单击“下一步”按钮将提示设置入站设置选项，如图 2-13 所示。入站身份验证方法主要用于设置当网络用户访问当前计算机时需要使用哪种身份验证方法。如果设置了“出站身份验证方法”则不会出现该对话框。

(12) 单击“下一步”按钮，显示如图 2-14 所示的“注册表设置摘要”对话框，显示了当前安全策略中所做的注册表安全设置。

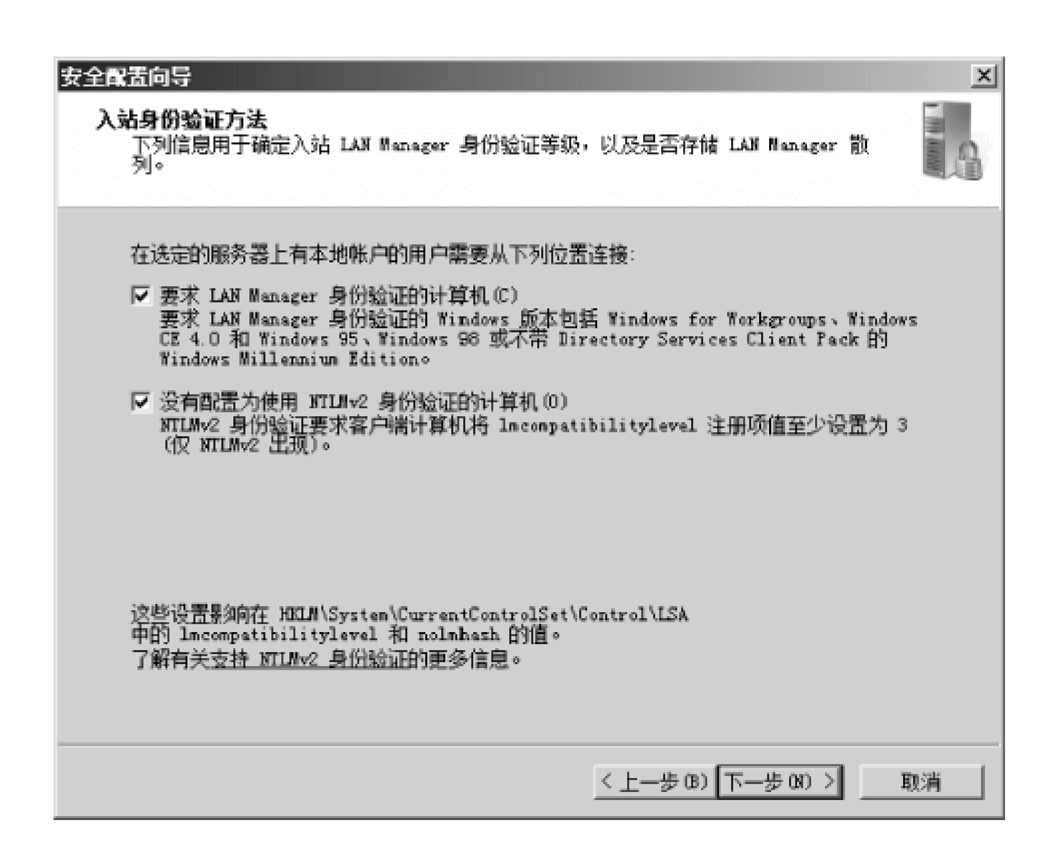


图 2-13　“入站身份验证方法”对话框

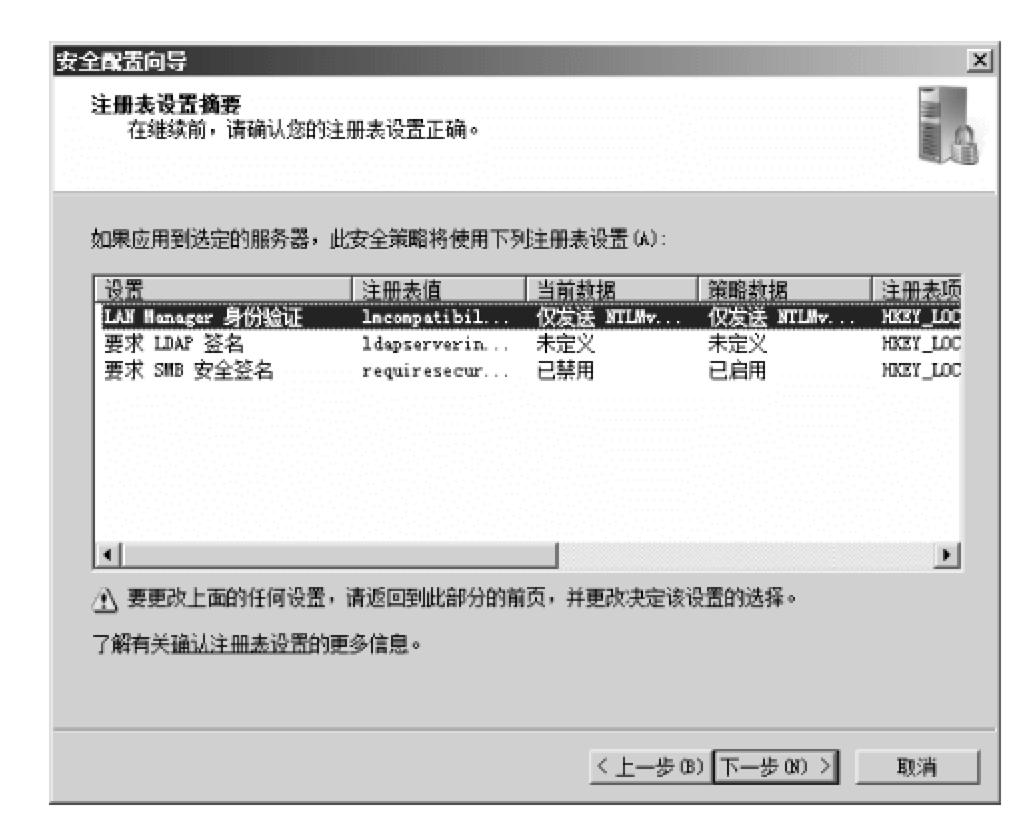


图 2-14　“注册表设置摘要”对话框

(13) 单击“下一步”按钮，显示“审核策略”对话框。Windows 审核策略主要用于审核日志记录中的相关内容，并确定受影响的系统对象。安全策略回滚功能是无法回滚安全向导中的审核策略设置的。单击“下一步”按钮，显示“系统审核策略”对话框。选择需要审核的目标，选中“审核成功的操作”单选按钮，即只审核日志记录中操作成功的事件记录，如图 2-15 所示。



图 2-15 “系统审核策略”对话框

(14) 单击“下一步”按钮，显示如图 2-16 所示的“审核策略摘要”对话框。列表中列出了应用策略时，将在选定服务器上对审核策略进行审核。此页显示每个审核策略设置的当前设置和由策略定义的设置。

(15) 单击“下一步”按钮，显示“保存安全策略”对话框。保存之后，即可将该安全策略应用到当前或其他服务器上。单击“下一步”按钮，显示如图 2-17 所示的“安全策略文件名”对话框。在保存安全策略文件的路径之后输入安全策略文件名，根据需要输入相关描述信息。

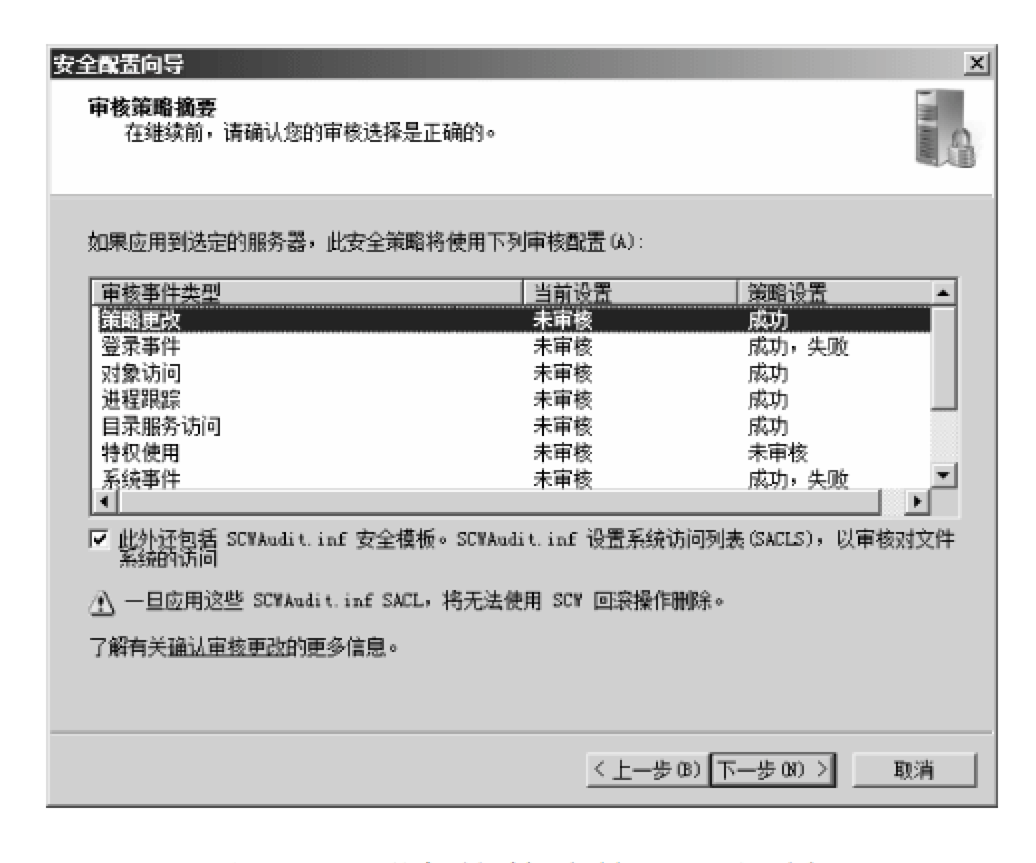



图 2-16 “审核策略摘要”对话框

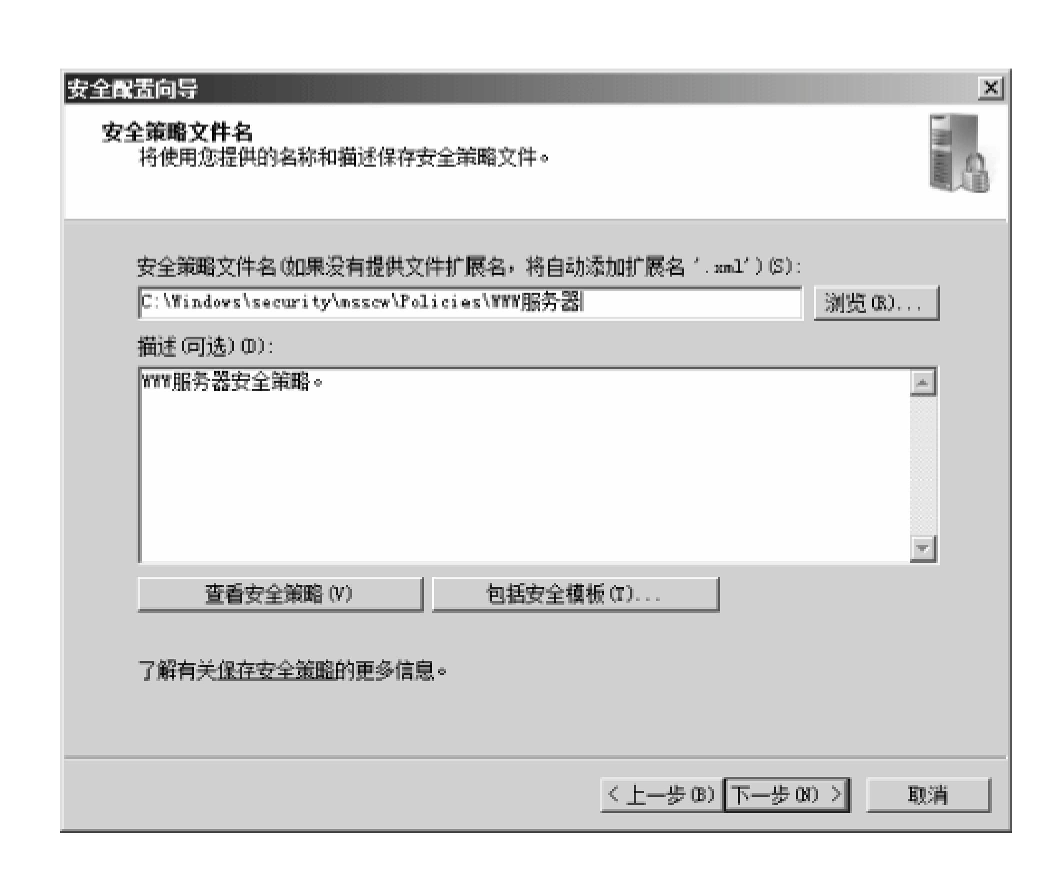


图 2-17 “安全策略文件名”对话框

提示：单击“包括安全模板”按钮，还可以向当前安全策略中添加其他安全模板中的安全规则，这些规则将拥有较高的优先级。SCW 回滚功能将无法回滚已经应用的策略模板中的规则设置。

(16) 单击“下一步”按钮，显示“应用安全策略”对话框。如果选中“现在应用”单选按钮，则可以将安全策略立即应用到当前服务器；建议选中“稍后应用”单选按钮，测试之后再

应用到服务器。单击“下一步”按钮，显示“正在完成安全配置向导”对话框。单击“完成”按钮，完成安全策略的设置，如图 2-18 所示。



图 2-18　完成安全配置向导

2.2.2　应用安全配置策略

应用安全配置策略的具体步骤如下。

(1) 依次选择“开始”→“管理工具”→“安全配置向导”选项，启动“安全配置向导”，单击“下一步”按钮，在“配置操作”对话框中，选中“应用现有安全策略”单选按钮，在“现有安全策略文件”文本框中输入安全策略文件的路径，也可单击“浏览”按钮查找，如图 2-19 所示。



图 2-19　应用安全配置策略

(2) 单击“下一步”按钮，显示如图 2-20 所示的“选择服务器”对话框，在“服务器”文本框中，输入想要应用到的服务器名称或 IP 地址。如果目标服务器为远程主机，则应单击“指定用户账户”按钮，选择连接到指定主机部署安全策略使用的用户账户及凭证。

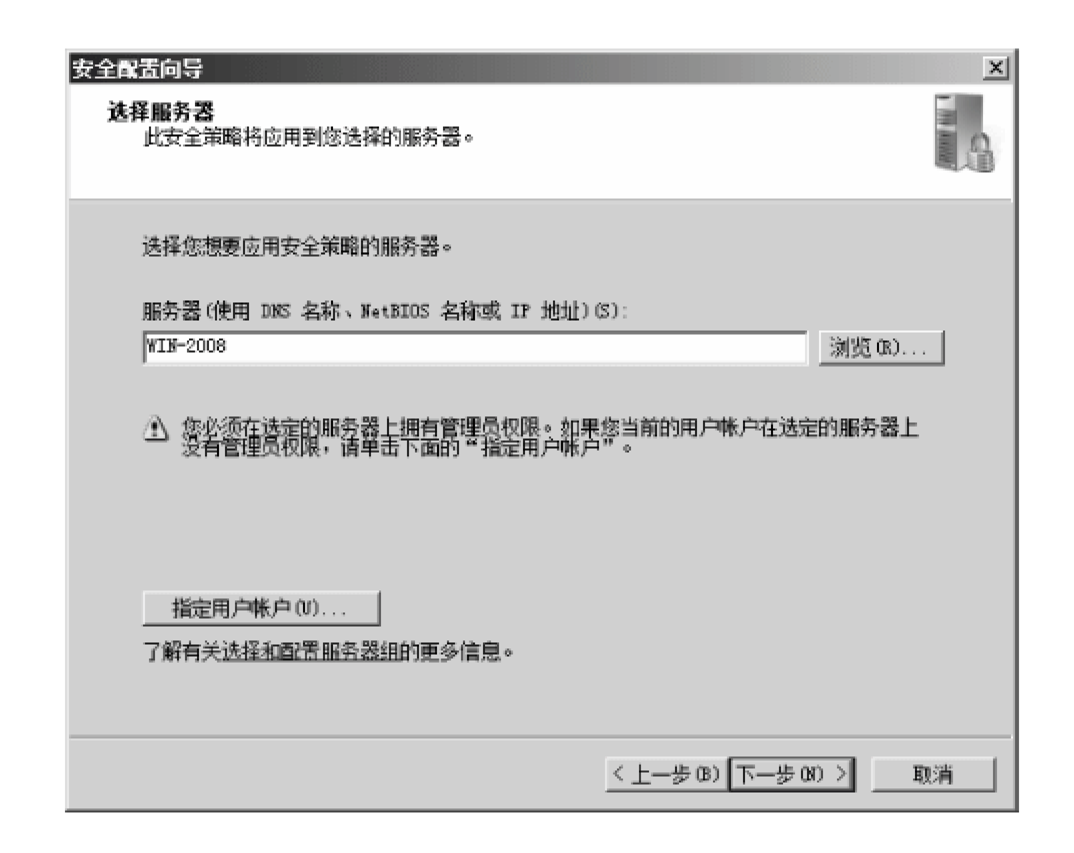


图 2-20 “选择服务器”对话框

(3) 单击“下一步”按钮,显示如图 2-21 所示的“应用安全策略”对话框,在“安全策略描述”信息框中显示的是该策略的相关描述信息,也可以单击“查看安全策略”按钮打开“SCW 查看器”窗口,查看其详细信息。单击“下一步”按钮,显示“正在应用安全策略”对话框。将安全策略应用到本地计算机大概需要几分钟时间,应用到远程计算机时所需时间可能更长一些。



图 2-21 “应用安全策略”对话框

(4) 单击“下一步”按钮,显示如图 2-22 所示的“正在完成安全配置向导”对话框。单击“完成”按钮,关闭安全配置向导。重新启动计算机后,应用的安全策略即可生效。

2.2.3 知识链接:安全配置向导

安全配置向导(Security Configuration Wizard,SCW)是从 Windows Server 2003 SP1 系统开始提供的功能,主要用于快速配置服务器系统安全。配置和应用 SCW 时应注意以下几点。

（1）SCW 禁用不需要的服务并提供对具有高级安全性的 Windows 防火墙的支持。

（2）使用 SCW 创建的安全策略与安全模板不同，其中前者扩展名为.xml，而后者扩展名为.inf。用户创建的安全策略源于安全模板，安全模板包含的安全设置可以应用于所有的服务器角色。

（3）部署 SCW 安全策略后并不会影响服务器提供服务时所需的组件，并且应用之后，管理员仍可以通过服务器管理器安装所需的组件。

（4）应用 SCW 安全策略之后，SCW 将自动选择所有从属角色。



图 2-22　“正在完成安全配置向导”对话框

（5）创建和应用 SCW 安全策略时，应确保服务器的 IP 协议及端口配置完全正确。

（6）大规模应用安全策略之前必须经过严格测试，确认可行之后方可部署。

（7）应用安全配置策略之后，必须重新启动计算机才可以生效。

2.3　配置 Windows 系统安全

无论是服务器操作系统，还是客户端 PC 操作系统，都是按照默认方式和设置安装的，这本身就存在很大的安全隐患，因此必须进行安全配置，以确保系统的安全性。

2.3.1　Windows Update

1. 配置 Windows Update

默认情况下，Windows Server 2008 安装完成后，自动更新功能是未配置的，管理员必须开启并指定选择相应的方式，为系统下载、安装补丁更新，以保护系统的安全。

（1）为 Windows Server 2008 配置系统更新之前，每次启动计算机后都会在任务栏的右侧系统托盘中，显示如图 2-23 所示的提示信息。

（2）单击此提示信息，打开如图 2-24 所示的 Windows Update 对话框。除此之外，在“初始配置任务”窗口的“更新此服务器”选项区域，以及在“服务器管理器”窗口的“安全信息”选项区域中，同样可以启动 Windows Update 配置向导。



图 2-23　此时未自动安装更新

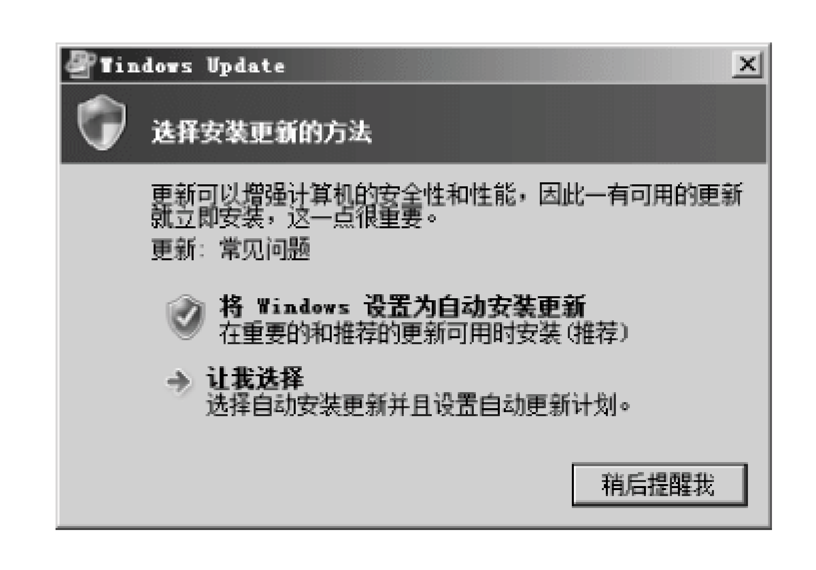


图 2-24　Windows Update 对话框

提示：只有第一次配置自动更新时才会显示该对话框，以后将不再显示。如果要让Windows系统自动下载并安装更新，可直接单击“将Windows设置为自动安装更新”按钮，完成系统更新配置。

(3) 单击“让我选择”按钮，打开如图2-25所示的“更改设置”对话框。在“选择Windows安装更新的方法”中，选择一种安装方法即可，各种安装方式的具体含义如下。



图 2-25 “更改设置”对话框

① 自动安装更新（推荐）：服务器连接到Internet后，系统将自动检测Microsoft Update服务器是否有所需更新，如果有则将自动下载并安装这些更新。选中该单选按钮后还需要指定系统自动安装更新的具体时间。

② 下载更新，但是让我选择是否安装更新：仅下载所需的系统更新，完成后通知用户在合适的时间手动安装。

③ 检查更新，但是让我选择是否下载和安装更新：仅检测Microsoft Update服务器上提供的更新项目，并以列表方式提示系统管理员，管理员可以根据实际情况选择需要下载的系统更新。建议使用这种方式，可以减少不必要的服务器资源和网络带宽浪费。

④ 从不检查更新（不推荐）：关闭系统更新功能，建议不要选择此项。

2. 安装系统更新

如果用户选择了“计划安装”方式，则安装向导将自动下载并安装系统更新，只是在必要时会提示重新启动计算机。

(1) 依次选择“开始”→Windows Update选项，显示如图2-26所示的Windows Update窗口，提示更新的数量和大小。

(2) 单击“查看可用更新”链接，显示如图2-27所示的“查看可用更新”窗口，不需要的更新可以直接取消其前面的复选框，如果不希望系统再次提示安装取消的更新，则右击该更新并选择快捷菜单中的“隐藏”选项即可。

(3) 单击“安装”按钮，或者在Windows Update窗口中单击“安装更新”按钮，显示如图2-28所示的窗口，开始下载并安装指定更新（与管理员设置的更新方式有关）。



图 2-26　Windows Update 窗口

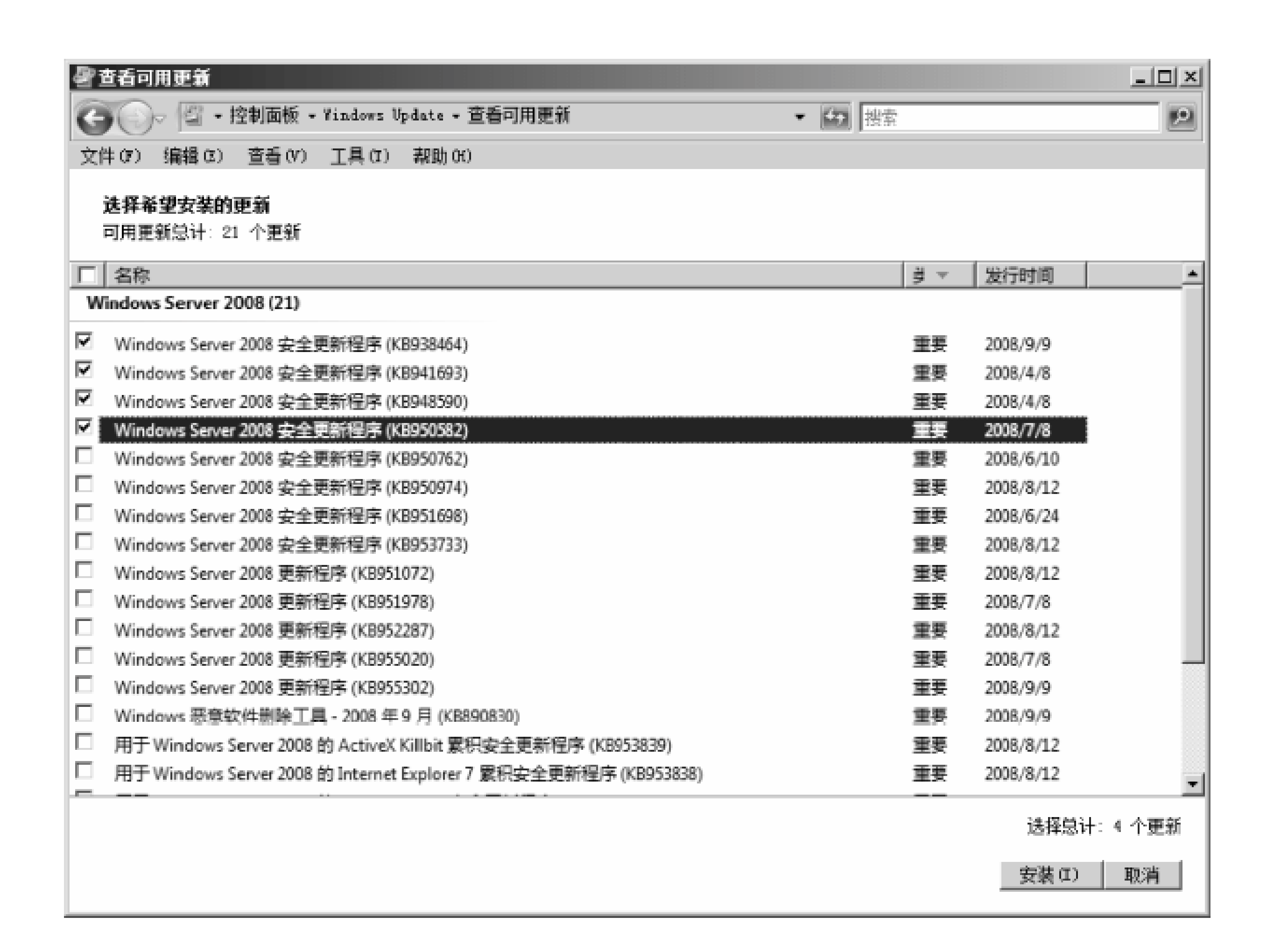


图 2-27　“查看可用更新”窗口



图 2-28　正在下载和安装

(4) 安装完成后，显示如图 2-29 所示的窗口，安装结果中包括安装成功或失败的数量，以及是否需要重新启动计算机。如果安装的更新涉及的应用程序正在运行，则可能导致安装失败。



图 2-29　安装完成

(5) 某些更新必须在重新启动系统后方可生效，此时，可以单击“立即重新启动”按钮重启计算机，也可以稍后再重新启动。系统默认，等待 10 分钟后自动显示如图 2-30 所示的对话框。在“请在以下时间段之后提醒我”下拉列表框中选择等待的时间，如“10 分钟”、“1 小时”、“4 小时”等。

(6) 单击“推迟”按钮，即可在指定时间后再次收到该提示信息，根据实际情况选择“立即重新启动”或“推迟”按钮即可。

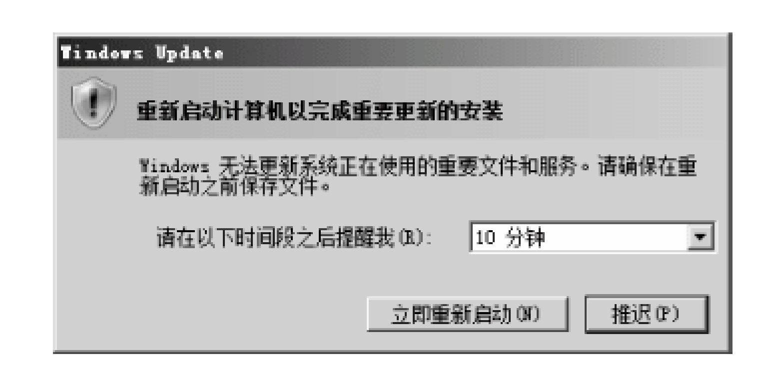


图 2-30　Windows Update 对话框

2.3.2　管理系统管理员账户

1. 更改 Administrator 账户名称

以 Administrator 账户登录本地计算机，依次选择“开始”→“管理工具”→“本地计算机管理”选项，打开“计算机管理”窗口，展开“系统工具”→“本地用户和组”→“用户”选项，右击 Administrator 账户并选择“重命名”选项，输入新的账户名称即可，如图 2-31 所示。设计新的账户名称时，尽量不要使用 Admin、master、guanliyuan 之类的名称，否则账户安全性同样没有任何保障。

域中的所有用户账户默认都是存放在域控制器的 Users 容器中的，Administrator 账户是整个域的超级管理员用户。依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开如图 2-32 所示的“Active Directory 用户和计算机”窗口，在 Users 容器中右击 Administrator 账户，并选择快捷菜单中的“重命名”选项即可。

输入新的账户名并确认时，会显示如图 2-33 所示的“Active Directory 域服务”对话框，建议更改之后立即注销并使用新的账户名登录，以避免出现访问冲突。单击“是”按钮，关闭

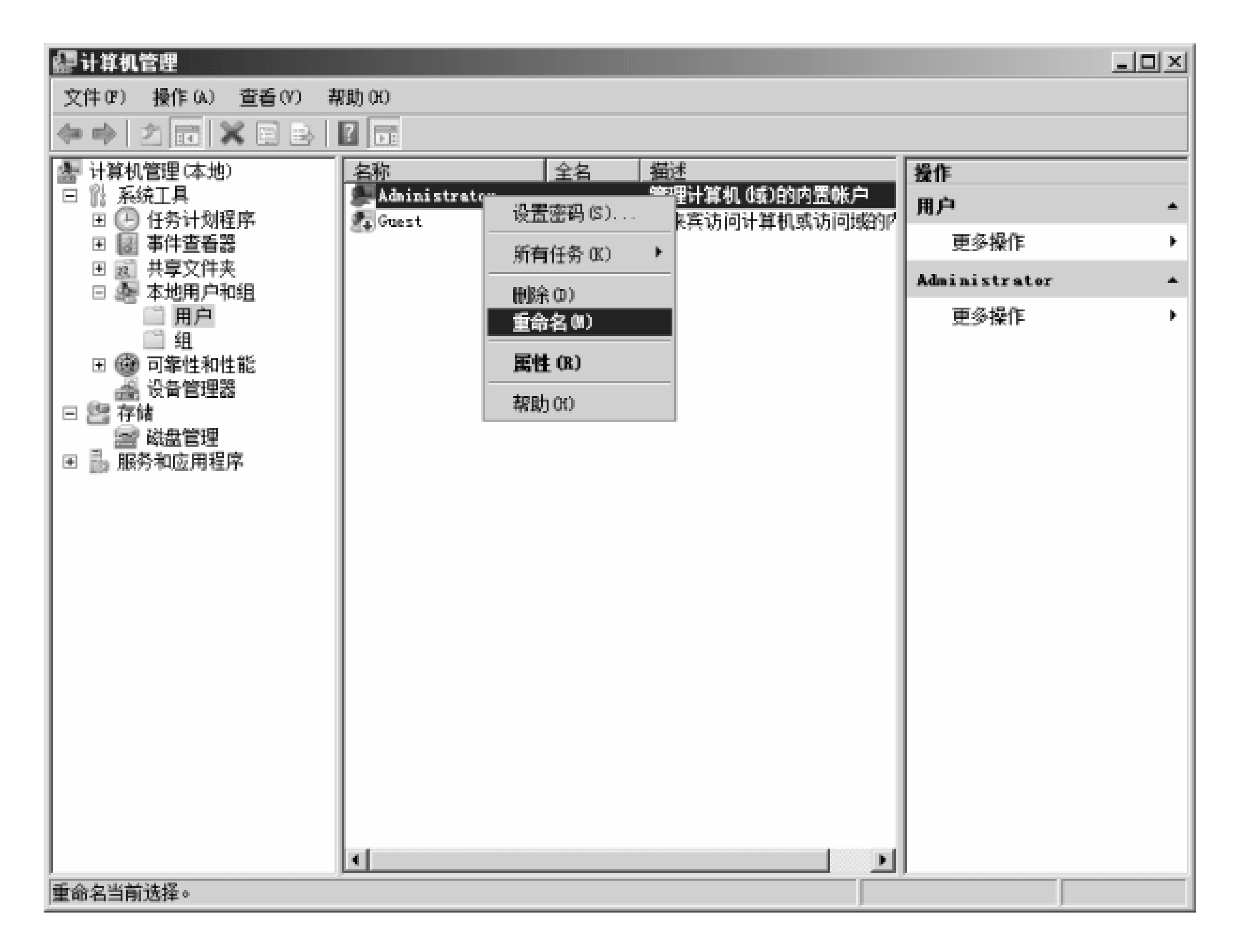


图 2-31　“计算机管理”窗口



图 2-32　“Active Directory 用户和计算机”窗口

该对话框，稍后注销当前用户账户即可。

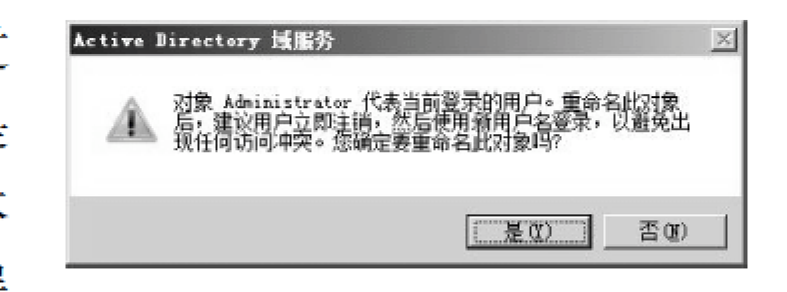


图 2-33　“Active Directory 域服务”对话框

无论是独立计算机还是域控制器，都可以通过 Windows 组策略更改 Administrator 账户名称。如果是独立计算机，则可以依次选择“开始”→“管理工具”→“本地安全策略”选项，打开“本地安全策略”控制台；依次展开“安全设置”→“本地策略”→“安全选项”选项，在右侧主窗口中双击“账户：重命名系统管理员账户”，打开“账户：重命名系统管理员账户 属性”对话框，如图 2-34 所示。重新输入新的账户名称即可。

如果是域控制器，则需要依次选择“开始”→“管理工具”→“组策略管理”选项，找到作用于根域的默认策略 Default Domain Policy，右击并选择快捷菜单中的“编辑”选项，打开“组策略管理编辑器”窗口，依次展开“策略”→“Windows 设置”→“安全设置”→“本地策略”→



图 2-34　通过本地安全策略更改管理员账户名

“安全选项”选项，双击右侧主窗口中的“账户：重命名系统管理员账户”，打开“账户：重命名系统管理员账户 属性”对话框，系统默认是没有定义该策略的，选中“定义这个策略设置”复选框，并在文本框中输入新的名称即可，如图 2-35 所示。



图 2-35　通过域安全策略更改管理员账户名

2. 创建陷阱账号

(1) 创建一个名称为 Administrator 的用户账户(如果原有管理员账户没有被更名则可以创建一个名称类似的账户，如 Admin 等)，并输入一个复杂程度极高的安全密码，选中“密码永不过期”复选框，如图 2-36 所示。



图 2-36　创建陷阱账户

(2) 单击“创建”按钮，即可创建该账户。

(3) 将其从 Users 组中删除，即可避免其集成来自 Users 组的用户权限，如图 2-37 所示。选择陷阱账户 Administrator 并单击“删除”按钮，将其删除。最后单击

“确定”按钮保存。

(4) 双击陷阱账户，打开用户账户属性对话框，将其各种权限设置为最低。例如，在“拨入”选项卡中选中“拒绝访问”单选按钮，如图 2-38 所示。



图 2-37　删除 Users 组中的陷阱账户

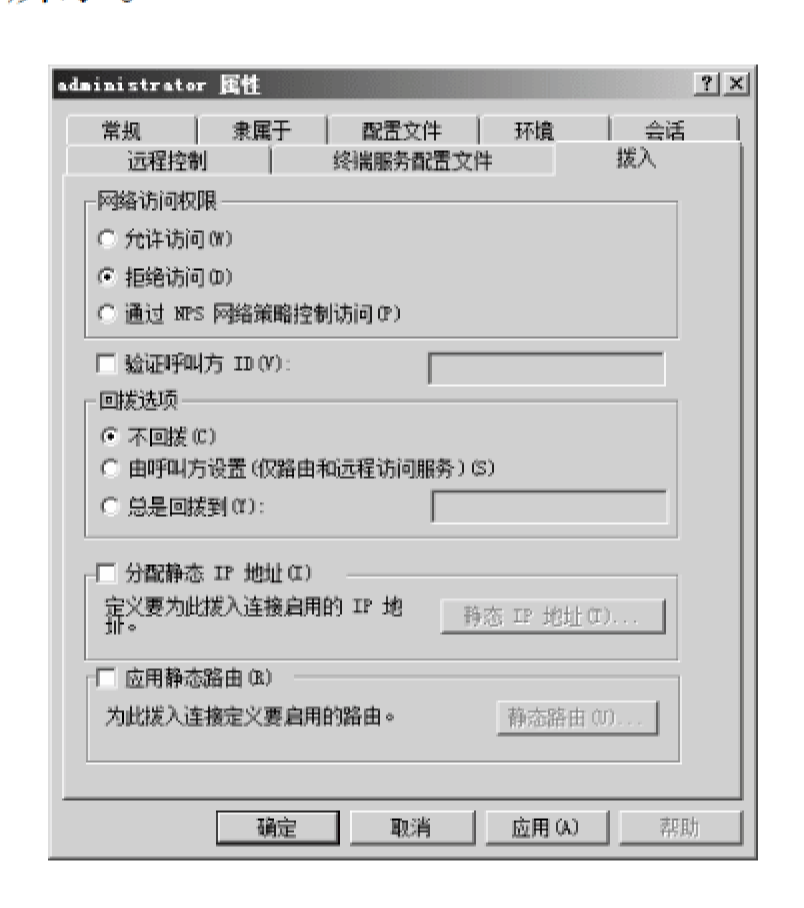


图 2-38　限制陷阱账户的权限

(5) 单击“确定”按钮，保存设置。

提示： 除此之外，还可以在所有磁盘分区的 NTFS 权限列表中一一删除陷阱账户的各种权限。总之，使其不具备任何操作权限，即使被盗用也无法进行任何破坏操作。

2.3.3　用户密码安全设置

入侵者若想盗取系统内的重要数据信息或执行某项管理功能，就必须先获得管理员权限，即破解管理员账户密码。密码破解软件工作机制主要包括 3 种：巧妙猜测、词典攻击和自动尝试字符组合。从理论上讲，只要有足够时间，使用这些方法可以破解任何账户密码，破解一个弱密码可能只需几秒钟即可完成，而要破解一个安全性较高的强密码则可能需要几个月甚至几年的时间。因此，系统管理员账户必须使用强密码，并且经常更改密码。

1. 注意事项

在设置管理员账户密码时，应注意以下问题。

(1) 不可使账号与密码相同。如果将用户账号与密码设置为相同，在一定范围内账户是公开的，而此时的密码也就毫无安全可言。

(2) 不可使用管理员姓名或企业名称。使用管理员的姓名或者企业名称作为密码，实在是不堪一击，对于本单位和熟悉本单位的人而言，各种容易想到的名称无疑是攻击的首选。另外，在许多黑客编写的字典中，往往将百家姓一一列出，并放在字典的前列。

(3) 不可使用英文词组。常用英文单词或词组虽然便于记忆，但这同样是黑客攻击字典不会错过的，因此安全性不高。

(4) 不可使用特定意义的日期。以具有特定意义的日期作为密码是任何人都十分喜爱的，这一类日期通常有自己生日、父母生日、儿女生日、朋友生日、重大节日、个人纪念日等。不仅很容易被熟悉的人猜到，即使是陌生人也可以通过穷举的方式而得手。

(5) 切不可使用简短的密码。简短密码便于记忆，破解起来也更加不堪一击。一个穷

举软件每秒钟可以重试10万次之多，字数越少，字符越简单化，排列组合的结果也就越少，也就越容易被攻破。

2. 安全密码原则

若欲保证账户密码的安全，应当遵循以下规则。

(1) 用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符，将这些符号排列组合使用，以期达到最好的保密效果。

(2) 用户密码不要太规则，不要将用户姓名、生日和电话号码作为密码。不要用常用单词作为密码。

(3) 根据黑客软件的工作原理，参照密码破译的难易程度，以破解需要的时间为排序指标，密码长度设置时应遵循7位或14位的整数倍原则。

(4) 在通过网络验证密码过程中，不得以明文方式传输，以免被监听截取。

(5) 密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上并包含密码的文件是只读的。加密的方法很多，如基于单向函数的密码加密，基于测试模式的密码加密，基于公钥加密方案的密码加密，基于平方剩余的密码加密，基于多项式共享的密码加密，基于数字签名方案的密码加密等。经过上述方法加密的密码，即使是系统管理员也难以得到。

(6) 密码应定期修改，应避免重复使用旧密码，应采用多套密码的命名规则。

(7) 建立账号锁定机制。一旦同一账号密码校验错误若干次即断开连接并锁定该账号，经过一段时间才解锁。

(8) 由网络管理员设置一次性密码机制，用户在下次登录时必须更换新的密码。

3. 系统账户密码要求

在Windows Server 2008系统中，安装系统的同时就要求管理员必须指定符合要求的安全密码，大大提高了用户账户和系统的安全性。通常情况下，Windows Server 2008网络中，对用户账户密码要求如下。

(1) 不包含全部或部分的用户账户名。

(2) 长度至少为6个字符。

(3) 包含来自以下4个类别中的3个的字符。

① 大写英文字母(从A～Z)。

② 小写英文字母(从a～z)。

③ 10个基本数字(从0～9)。

④ 非字母字符(例如，!、$、#、%)。

对于未安装Active Directory服务的Windows Server 2003计算机或修改了Windows Server 2003/2008默认组策略的计算机，其用户账户密码可以随意设置。

强密码具有以下特征。

(1) 长度至少有7个字符。

(2) 不包含用户的生日、电话、用户名、真实姓名或公司名等。

(3) 不包含完整的字典词汇。

(4) 包含全部下列4组字符类型。大写字母(A～Z)、小写字母(a～z)、数字(0～9)、非字母字符(`、～、!、@、#、$、%、^、&、*、(、)、_、+、－、=、{、}、|、[、]、\、:、"、;、'、<、

>、?、,、.、/)。

除此之外，管理员账户的密码应当定期修改，尤其是当发现有不良攻击时，更应及时修改复杂密码，以避免被破解。为避免密码因过于复杂而忘记，可用笔记录下来，并保存在安全的地方，或随身携带避免丢失。其实，最安全的方法就是不使用常规密码，而采用电子密钥等一些几乎无法破解的登录方式，确保系统安全性。

2.3.4　配置 Internet 连接防火墙

Internet 连接防火墙(Internet Connection Firewall，ICF)是 Windows 系统的内置防火墙，不仅可以阻止来自外部网络的恶意访问或攻击，还可以阻止当前服务器向其他计算机发送恶意软件。Windows Server 2008 系统的 ICF 默认情况下已经启动，管理员可以根据需要进行配置。如果服务器已经连接到网络，则网络访问策略的设置可能会阻止管理员对 Windows 防火墙的配置。

(1) 在 Windows Server 2008 的“控制面板”窗口中，双击“Windows 防火墙”图标，显示如图 2-39 所示的窗口。本例中的 Windows 防火墙已启用。



图 2-39　“Windows 防火墙”窗口

(2) 单击“启用或关闭 Windows 防火墙”链接，打开如图 2-40 所示的“Windows 防火墙设置”对话框，系统默认选中“启用”单选按钮。如果同时选中“阻止所有传入连接”复选框，则防火墙将阻止所有主动连接当前服务器的尝试，除非需要为该服务器提供最大限度的保护时，才使用该设置，启用该设置后将忽略“例外”列表中的所有设置。通常情况下，不推荐选中该复选框。

(3) 打开“例外”选项卡或者在“Windows 防火墙”窗口中，单击“允许程序通过 Windows 防火墙”链接，显示如图 2-41 所示的“例外”选项卡，在“程序或端口”列表中，选中该服务器欲提供的网络服务即可。

提示：在“高级安全 Windows 防火墙”工具中，也可以查看 Windows 防火墙的“例外”设置。

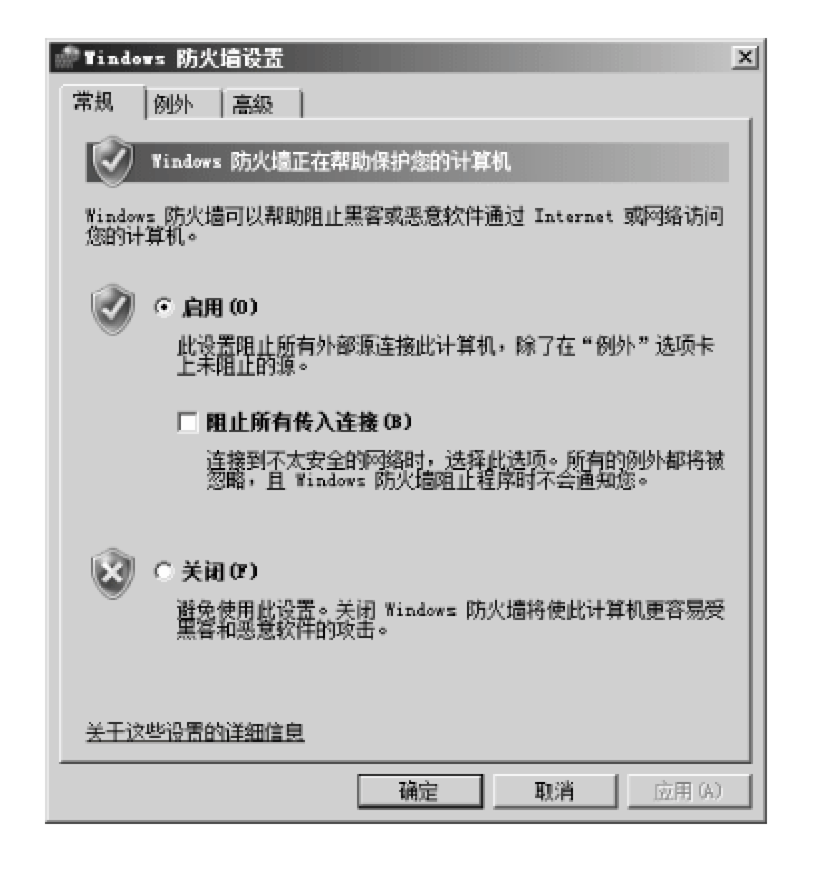


图 2-40 “Windows 防火墙设置”对话框



图 2-41 “例外”选项卡

(4) 单击“添加端口”按钮，打开如图 2-42 所示的“添加端口”对话框，即可向列表中增加新的网络服务所使用的 TCP 或 UDP 端口。在“名称”文本框中输入便于识别的名称，如 telnet；在“端口号”文本框中输入想要添加的端口，如 23；根据需要选择 TCP 或 UDP 端口类型。

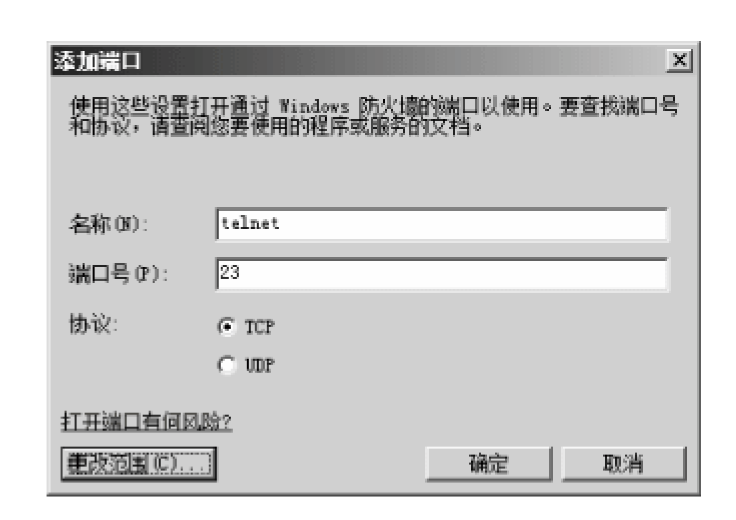


图 2-42 “添加端口”对话框

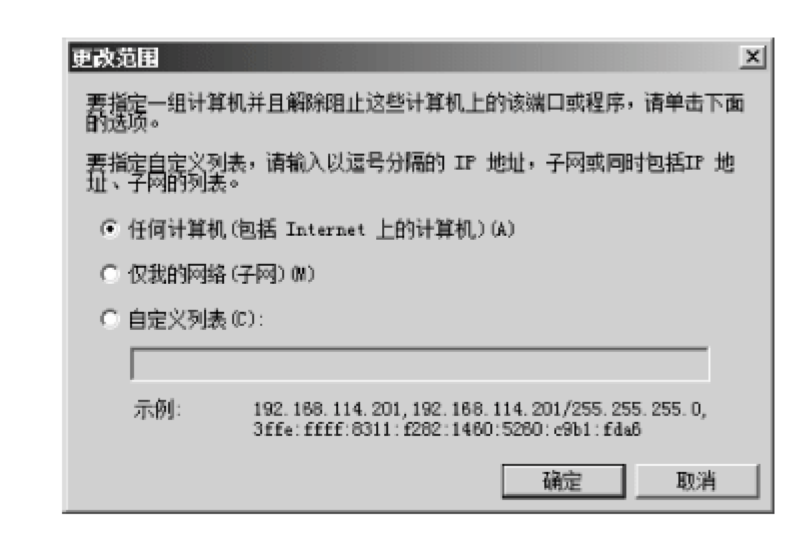


图 2-43 “更改范围”对话框

(5) 单击“更改范围”按钮，打开如图 2-43 所示的“更改范围”对话框。指定详细的限定范围可以提高防火墙策略的安全性。默认情况下，开放的防火墙端口适用于任何计算机（包括 Internet 上的计算机）。

提示：选中“仅我的网络（子网）”单选按钮，则开放端口仅适用于本地计算机所在子网，对其他用户仍然关闭。选中“自定义列表”单选按钮，则可以根据需要指定详细的 IP 地址或子网范围。

(6) 单击“高级”标签切换至如图 2-44 所示的“高级”选项卡，在“网络连接设置”选项区域，可以设置接受 Windows 防火墙保护的网络连接，默认为所有本地连接。在“默认设置”选项区域，单击“还原为默认值”按钮即可撤销所有 Windows 防火墙设置，恢复至初始状态。需要注意的是，必须是本地计算机上 Administrators 组的成员，或者是被委派了适当的权限的用户，才可以还原

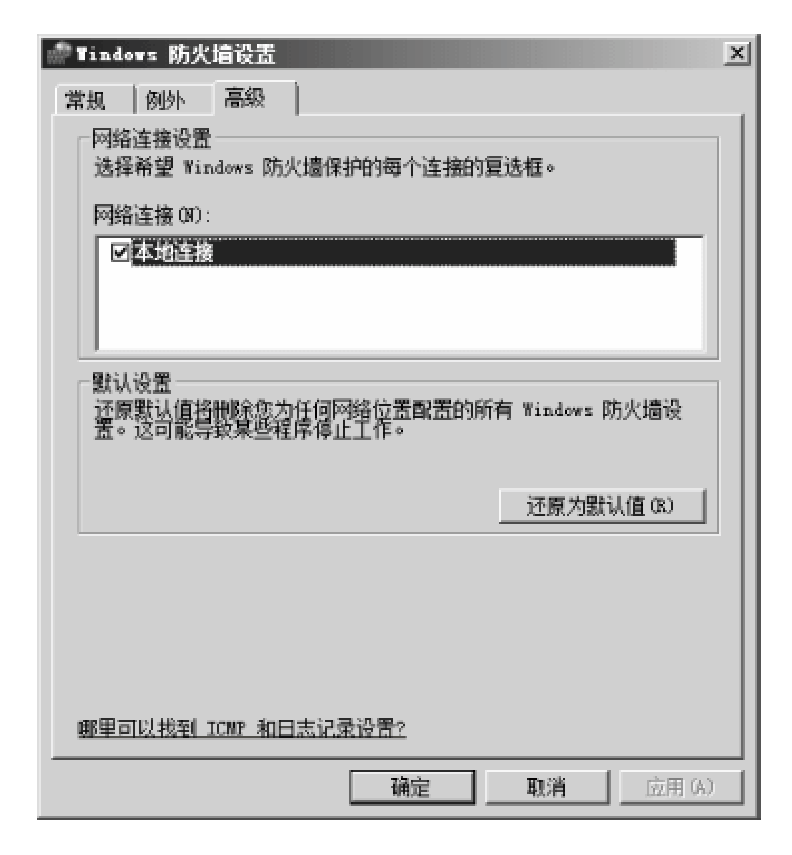


图 2-44 “高级”选项卡

Windows 防火墙默认设置。如果计算机已经加入到某个域中,则 DomainAdmins 组的成员可以执行该过程。

提示:与 Windows Server 2003 的 Internet 防火墙不同的是,“高级”选项卡中的 ICMP 相关设置,已被转移到“高级安全 Windows 防火墙”中。

(7) 单击“确定”按钮,保存设置即可。

2.3.5 配置默认共享

默认共享主要是为了方便网络管理员管理网络中的计算机,特别是在基于域的网络中,专门有几个默认共享用于存储用户配置文件是非常方便的。但是,默认共享在方便管理的同时,也给计算机的安全埋下了重大安全隐患。如果知道了管理员账户和密码,任何人都能访问计算机,所以如果管理员账户密码被恶意用户窃取,对于计算机的安全来说是非常不利的。

1. 查看默认共享

(1) 命令行方式

如果想要查看本地计算机目前所打开的默认共享,可以在本地计算机的命令提示符下,使用 net share 命令来查看系统目前所有的共享的目录。在这些所列出的共享目录中,不但包括默认共享,还包括系统除默认共享以外的所有共享目录。

在命令行提示符下,输入如下命令:

```
net share
```

按 Enter 键,命令成功执行,如图 2-45 所示。



图 2-45 net share 的执行结果

在这里所显示的就是系统的所有共享目录,这里主要包括 IPC$ 默认共享、逻辑磁盘共享 D$、C$,系统目录共享 ADMIN$。

(2) 图形窗口方式

如果用户对在命令提示符下的操作不是很熟悉,还可以使用图形方式,查看目前系统的默认共享目录。

以管理员账户登录系统,依次选择“开始”→“管理工具”→“计算机管理”选项,打开“计算机管理”窗口。依次展开“系统工具”→“共享文件夹”→“共享”选项,如图 2-46 所示。共

享列表中显示的就是本地计算机上已经设置的所有共享。



图 2-46　共享文件夹

2. 停止默认共享

(1) 使用 net share 命令

在命令行提示符下,输入如下命令:

```
net share d$ /delete
```

按 Enter 键,命令成功执行,即可停止共享,如图 2-47 所示。

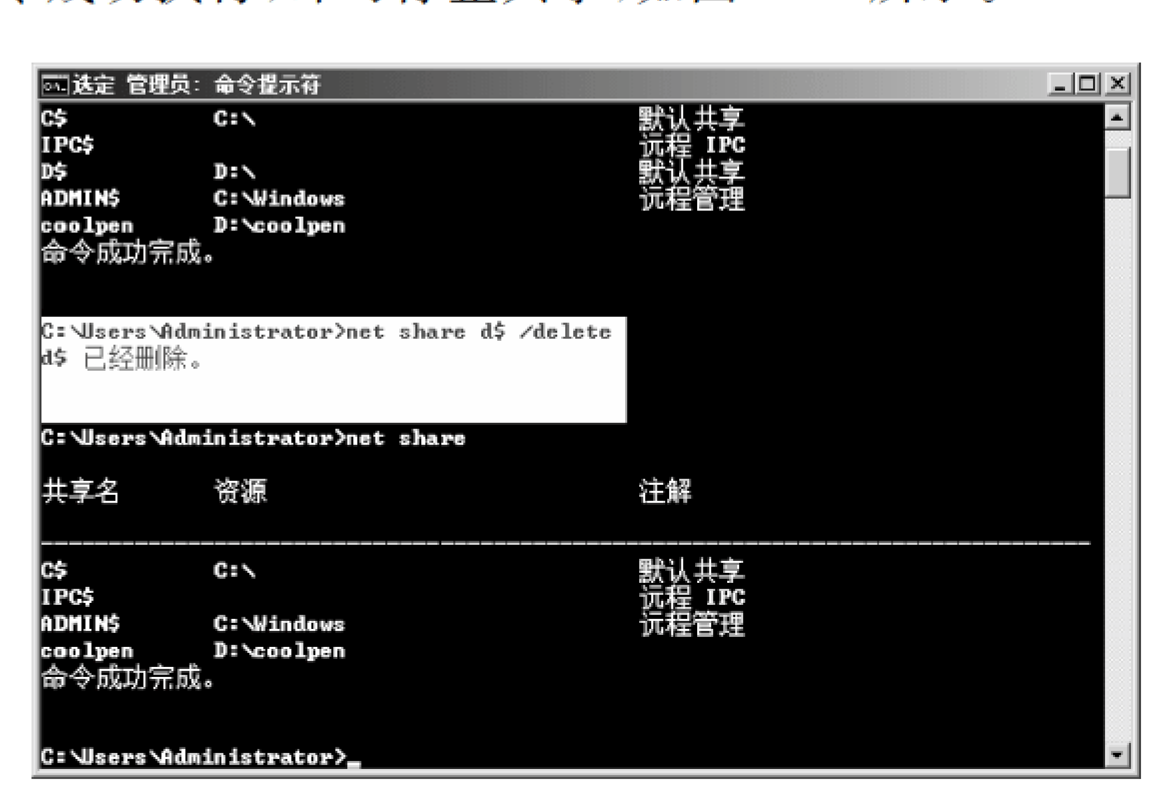


图 2-47　删除 D$ 默认共享

其中 D$ 表示系统默认共享 D 盘,其他如 C$、ADMIN$、IPC$ 等都可以使用此种格式删除。

在/delete 前必须要有空格。可以使用 net share ADMIN$ 或 net share IPC$ 建立 ADMIN$ 或 IPC$ 共享(如果共享存在,则为显示共享),但需要注意的是,其他共享则不能使用该方法来建立默认共享。

如果需要删除所有的默认共享,可以使用脚本命令(批处理文件方式)完成(即扩展名为.bat 的文件):

```
net share IPC$ /delete
```

```
net share Admin$ /delete
net share C$ /delete
net share D$ /delete
…
```

默认共享的盘符可以根据需要使用脚本命令分别删除，该批处理文件可以在命令提示符下运行，也可以将其添加到启动项中，如图 2-48 所示。这里创建一个名为 share. bat 的批处理文件，用以将系统的默认共享删除，并在命令提示符下运行。

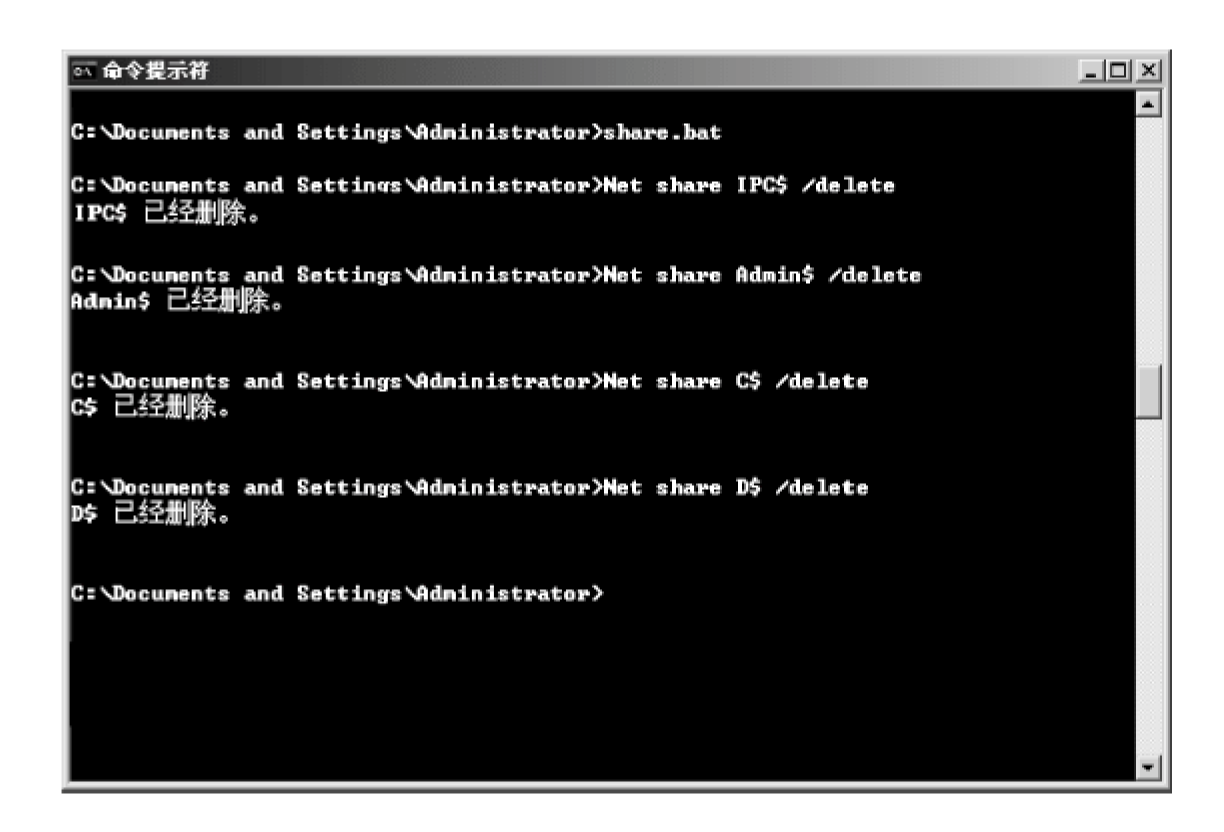


图 2-48 在命令提示符下运行批处理文件

（2）关闭 Server 服务

默认共享使用的是计算机系统的 Server 服务，如果将该服务直接关闭，就可以直接删除默认共享。

① 依次选择“开始”→“管理工具”→“服务”选项，打开“服务”窗口，双击 Server 服务，打开“Server 的属性(本地计算机)”对话框，如图 2-49 所示。在“启动类型”下拉列表框中，选择“手动”选项，以免再次重新启动系统时服务随之启动。

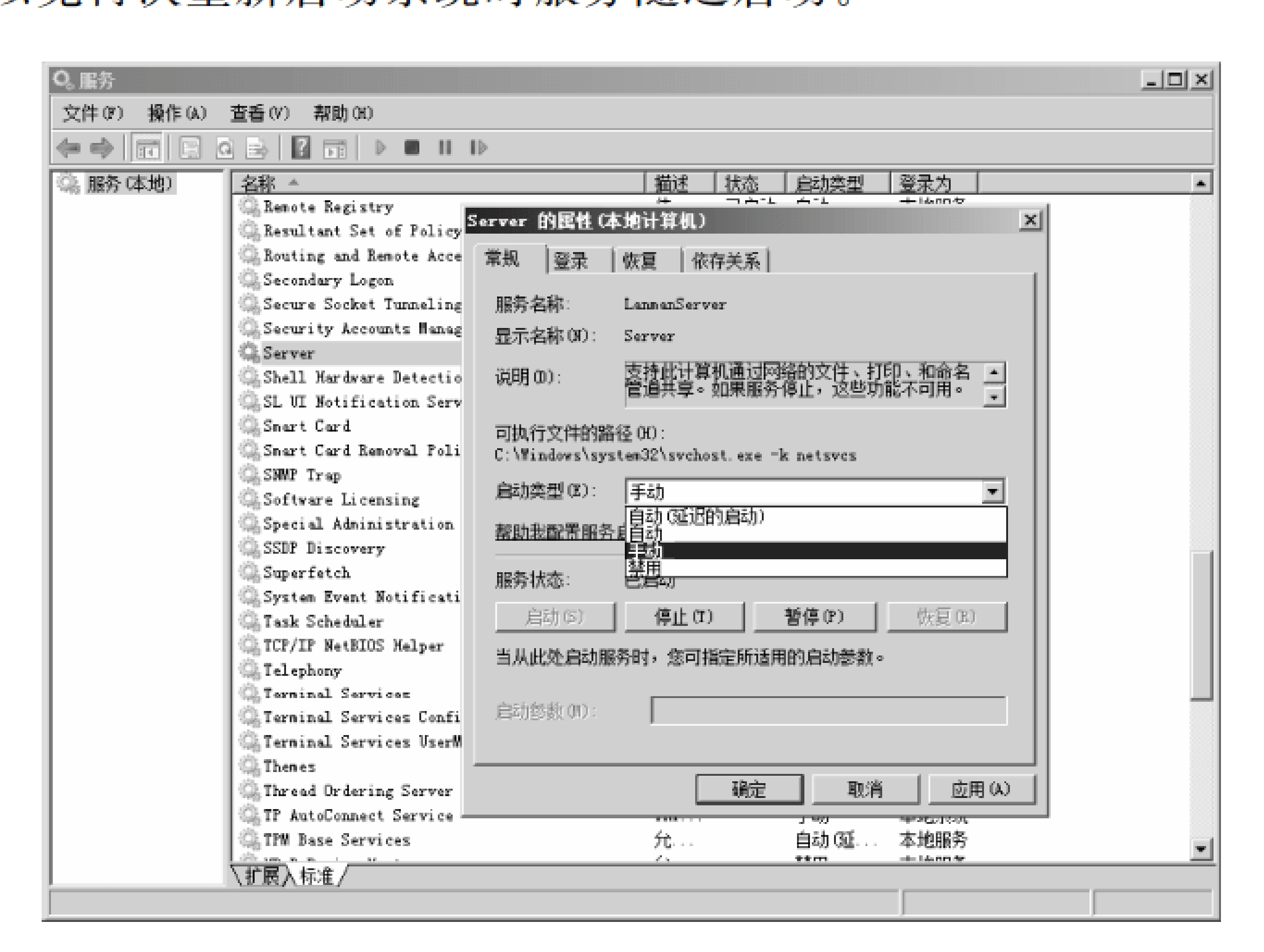


图 2-49 “Server 的属性(本地计算机)”对话框

② 单击“停止”按钮，开始停止 Server 服务。完成后单击“确定”按钮保存设置。再次打开命令提示符窗口，输入如下命令：

```
net share
```

按 Enter 键，显示如图 2-50 所示的结果，提示 Server 服务没有启动，直接输入 n 并按 Enter 键即可。

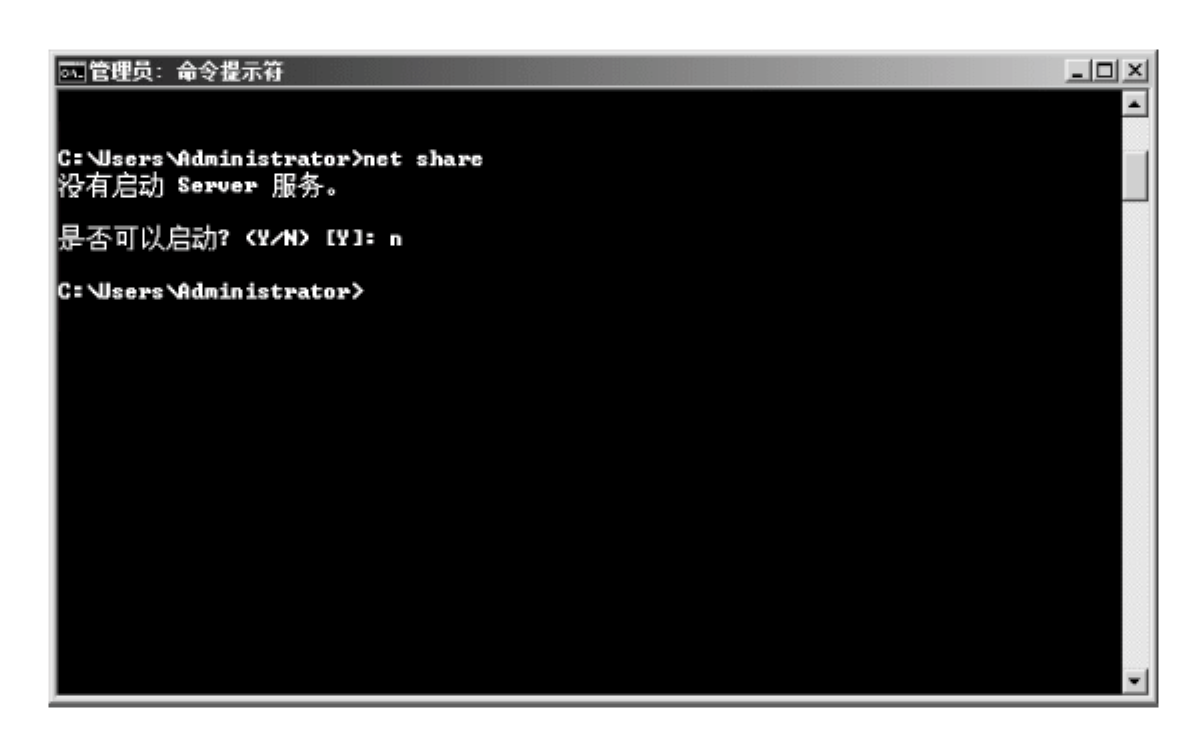


图 2-50　关闭 Server 服务后

使用这种方法停止默认共享后，其他共享也将同时被取消，应慎重选择。

(3) 修改注册表

使用前面两种方法完成停止系统默认共享，当系统重新启动后，默认共享会重新恢复。如果用户需要永久性地停止系统默认共享，可以通过修改注册表的方法来实现。停止系统默认共享的键值，默认情况下在 Windows 操作系统上不存在，需要用户手动添加该键值，修改后重新启动计算机即可使该键值生效。

① 单击“开始”按钮，在“开始搜索”文本框中，输入 regedit 并按 Enter 键，打开“注册表编辑器”窗口。依次展开如下注册表子项：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\AutotunedParameters，如图 2-51 所示。

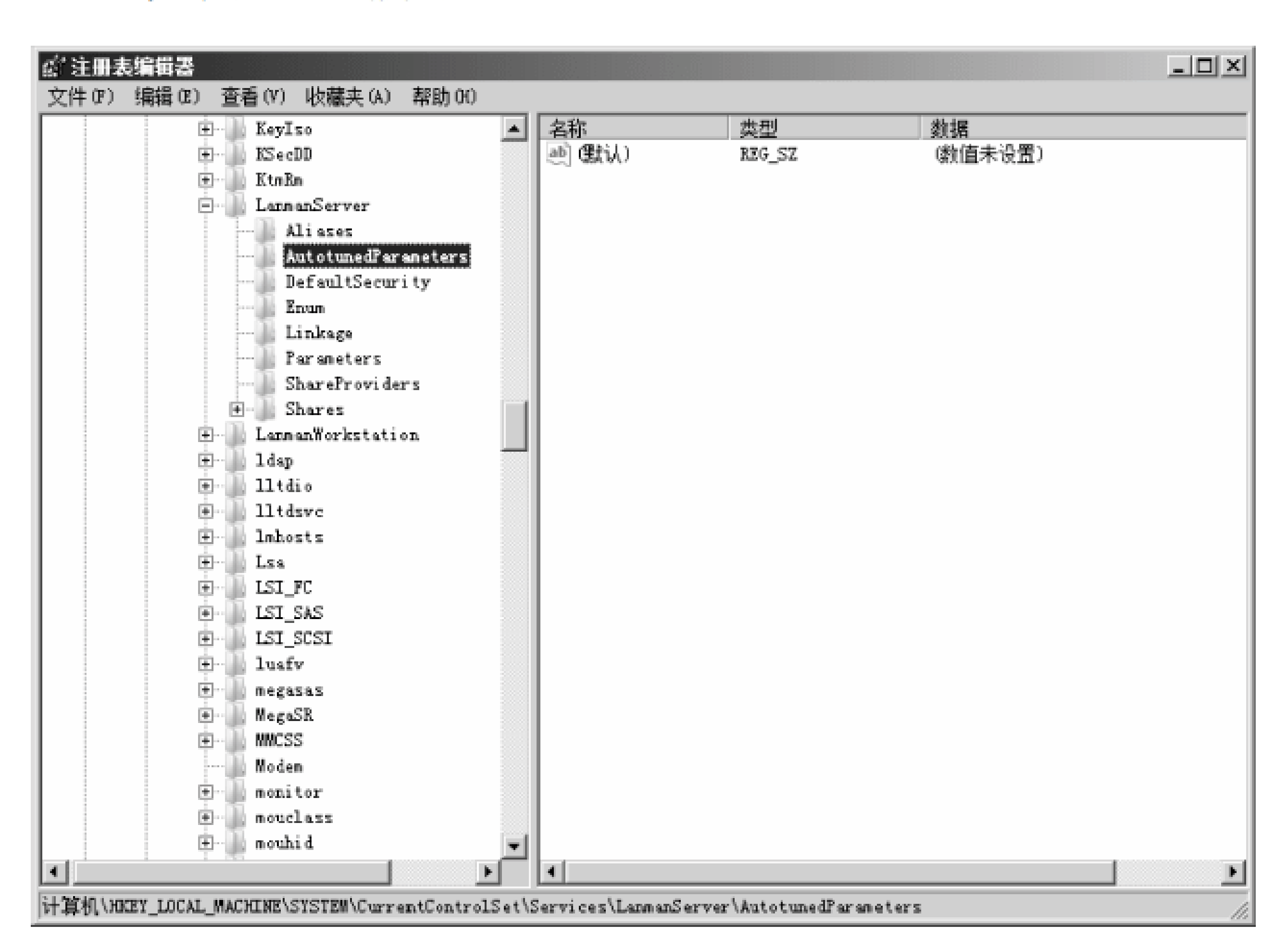


图 2-51　展开的注册表项目

② 在右侧的空白窗口中右击，在快捷菜单中选择“新建”选项，在子菜单中选择“Dword值”选项，新建一个名为 AutoShareServer 的 DWORD 值，并将其赋值为：00000000，如图 2-52 所示。

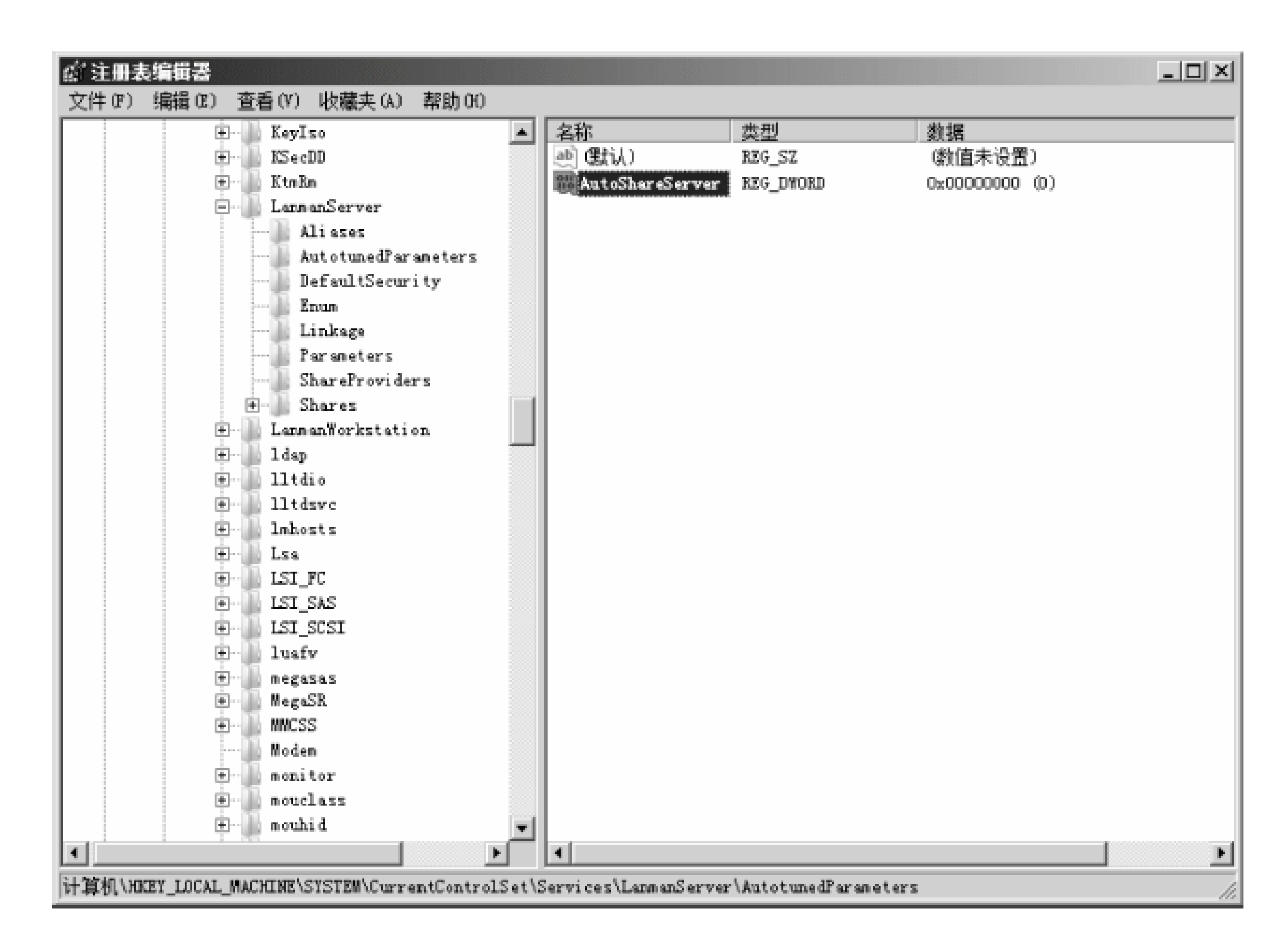


图 2-52 创建 DWORD 值

（4）Microsoft 网络的文件和打印机共享

除使用修改注册表的方法外，还可以使用卸载 TCP/IP 组件相关项目的方法，同样也可以关闭默认共享。

① 在“控制面板”窗口中，打开“网络和共享中心”窗口。单击“查看状态”按钮，打开“本地连接 状态”对话框，单击“属性”按钮，显示如图 2-53 所示的“本地连接 属性”对话框。

② 选中“Microsoft 网络的文件和打印机共享”复选框，单击“卸载”按钮，系统提示确认删除信息，显示如图 2-54 所示的“卸载 Microsoft 网络的文件和打印机共享”对话框。

③ 单击“是”按钮，即可完成“Microsoft 网络的文件和打印机共享”项目的卸载。



图 2-53 “本地连接 属性”对话框

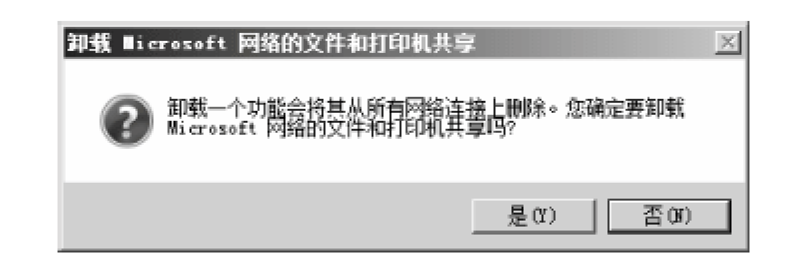


图 2-54 卸载信息提示

2.3.6 系统服务安全

系统服务对于服务器系统的重要性不言而喻,同时对于系统安全的意义也是非常重大的。所有系统应用都依赖于不同的服务,通过控制系统服务的状态,可以限制相应功能的开启或关闭,从而确保系统的安全。默认情况下,大多数系统服务的登录账户都是“本地系统账户”。如有特殊需要,可按照如下步骤更改为其他账户。

(1) 依次选择“开始”→“管理工具”→“服务”选项,打开“服务”窗口。双击需要更改登录账户的服务(如 Windows Installer 服务),打开服务属性对话框,切换至如图 2-55 所示的“登录”选项卡,默认选中“本地系统账户”单选按钮。

注意:*建议不要选中“允许服务与桌面交互”复选框。如果允许服务与桌面交互,则服务在桌面上显示的任何信息也都会显示在交互用户的桌面上。恶意用户可能会获得对该服务的控制权,或从交互桌面攻击它。*

(2) 选中“此账户”单选按钮,单击“浏览”按钮,打开“选择用户”对话框,在“输入要选择的对象名称(例如)”文本框中输入想要设置的登录账户,如图 2-56 所示。也可以单击“高级”按钮,从用户列表中搜索目标账户。

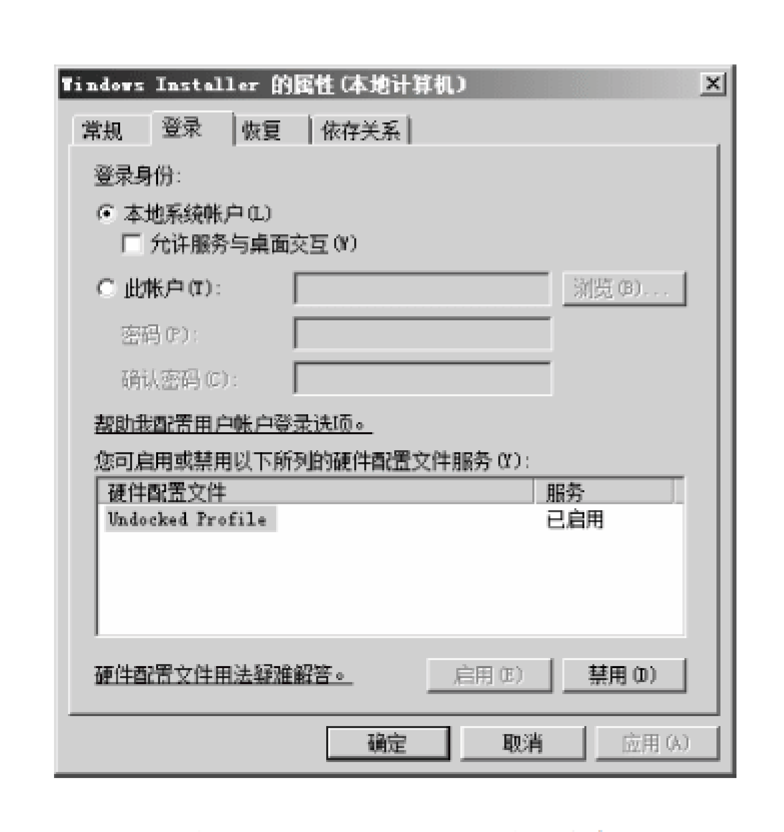


图 2-55 “登录”选项卡

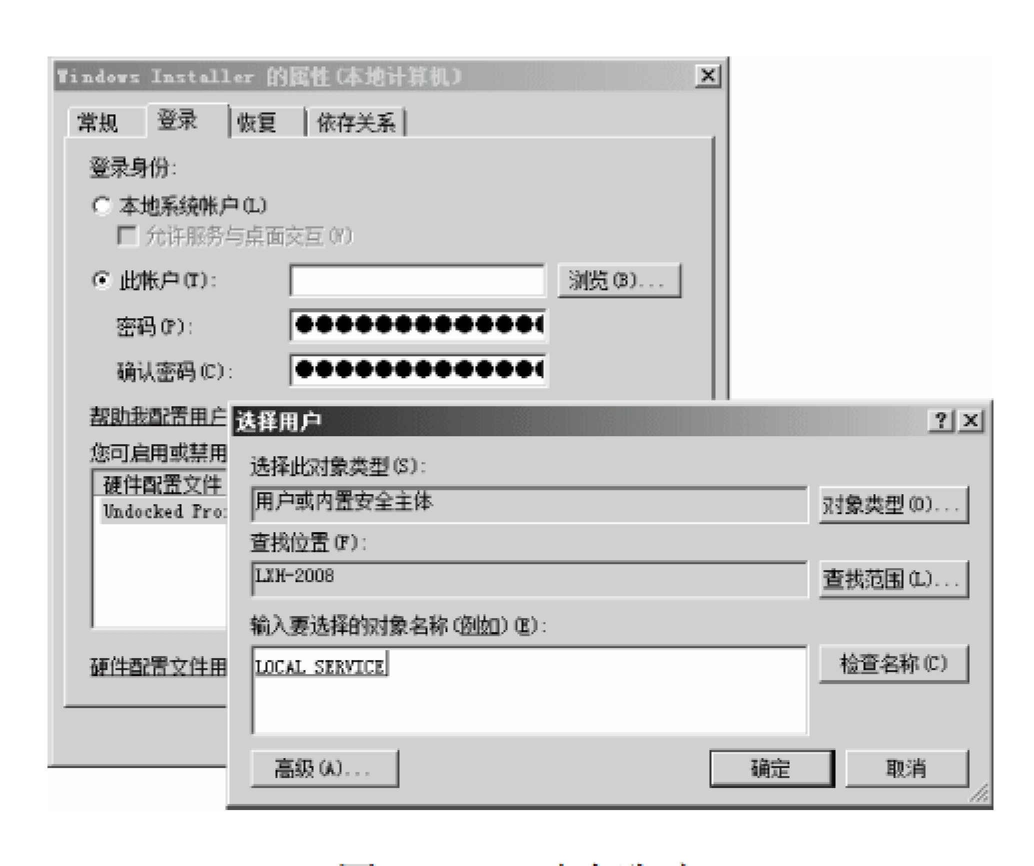


图 2-56 更改账户

(3) 单击“确定”按钮,即可将所选账户添加到“此账户”文本框中。本例中使用的 Local Service 账户,密码必须为空,如图 2-57 所示。如果选择其他账户,则在“密码”和“确认密码”文本框中输入用户账户的密码即可。

(4) 单击“应用”按钮,显示如图 2-58 所示的对话框,提示已经成功授予用户账户“以服务方式登录”的权利。

(5) 单击“确定”按钮,保存设置即可。需要注意的是,必须重新设置服务才可使更改生效。

2.3.7 用户账户控制

UAC 要求所有用户在标准账号模式下运行程序和任务,阻止未认证的程序安装,并阻止标准用户进行不当的系统设置改变。UAC 可以防止恶意软件获取特权,即使用户是以管理员账户登录的也可以起到保护作用。

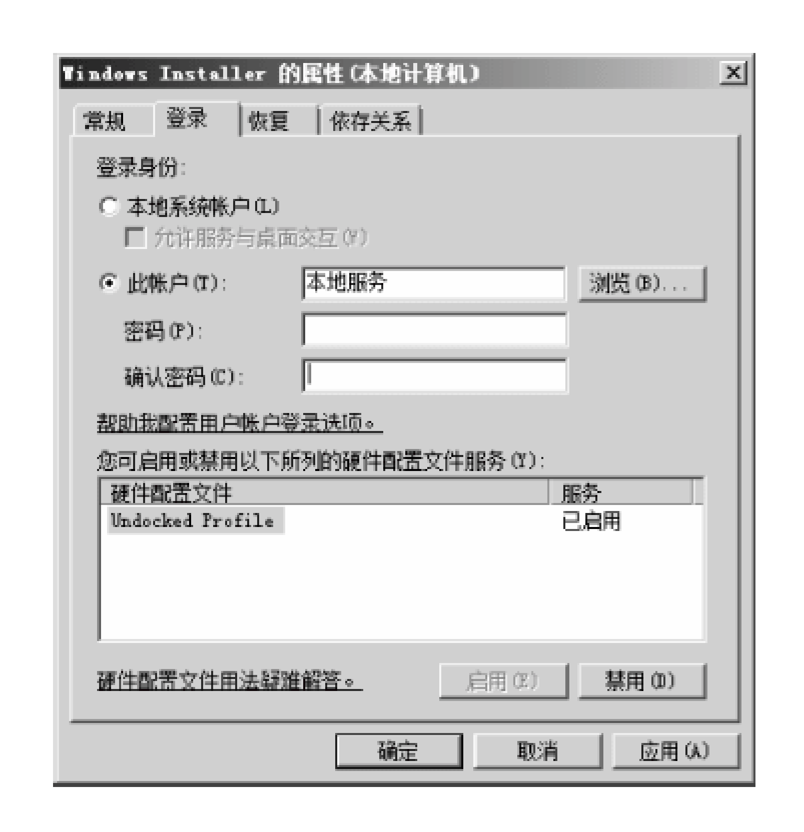



图 2-57 本地服务



图 2-58 登录账户更改成功

1. 开启或关闭用户账户控制

Windows Vista 系统的用户账户控制功能默认是开启的,建议保持开启状态。如果由于其他原因临时关闭,应按照如下方法重新开启。

(1) 在"控制面板"窗口(经典视图)中,双击"用户账户"图标,打开如图 2-59 所示的"用户账户"窗口。

(2) 单击"打开或关闭'用户账户控制'"链接,打开如图 2-60 所示的"打开或关闭'用户账户控制'"窗口,确保选中"使用用户账户控制(UAC)帮助保护您的计算机"复选框即可。



图 2-59 "用户账户"窗口



图 2-60 "打开或关闭'用户账户控制'"窗口

(3) 单击"确定"按钮,关闭窗口即可。开启"用户账户控制"功能后,非管理员账户执行某些操作时,就会出现如图 2-61 所示的"用户账户控制"对话框。通常情况下,当需要权限或密码才能完成任务时,UAC 会提示下列消息之一。

① Windows 需要您的许可才能继续。表示用户执行的操作可能会影响本地计算机其他用户的 Windows 功能或应用程序运行。

② 程序需要您的许可才能继续。表示用户执行的程序不属于 Windows 的一部分,系统要求指明其名称和发布者有效的数字签名,该数字签名可以帮助确保该程序正是其所声明的程序。

③ 一个未能识别的程序要访问您的计算机。未能识别的程序是指不具备发行者提供的数字签名的应用程序，此类程序存在一定的危险性，应该特别注意并且仅当其获取可信任资源时，才可以继续执行程序。

④ 此程序已被阻止。表明管理员已阻止当前账户在该计算机上运行指定的应用程序，若要继续执行，必须与管理员联系，并且请求其解除对此程序的阻止。



图 2-61 "用户账户控制"对话框

2. 设置"用户账户控制"提示信息

管理员还可以根据需要，设置"用户账户控制"功能中不同的提示消息和行为，例如需要允许其他用户账户暂时具有安装程序或执行某种操作的权限时，每一步操作都要提示"用户账户控制"信息，显然非常麻烦。此时，可通过修改"用户账户控制"使其可以直接操作，而不必提供管理员账户密码等凭证。需要注意的是，修改后可能会对系统安全性或用户的权限造成影响。

(1) 以本地计算机 Administrators 组中的成员账户登录系统，依次选择"控制面板"→"管理工具"→"本地安全策略"选项，在"本地安全策略"窗口中展开"本地策略"→"安全选项"选项，找到"用户账户控制"相关策略部分，如图 2-62 所示。

(2) 双击"用户账户控制：管理员批准模式中管理员的提升提示行为"策略，打开如图 2-63 所示的对话框，默认设置为同意提示。该策略主要用于限制，当用户执行需要经系统管理员批准的操作时的提示行为。

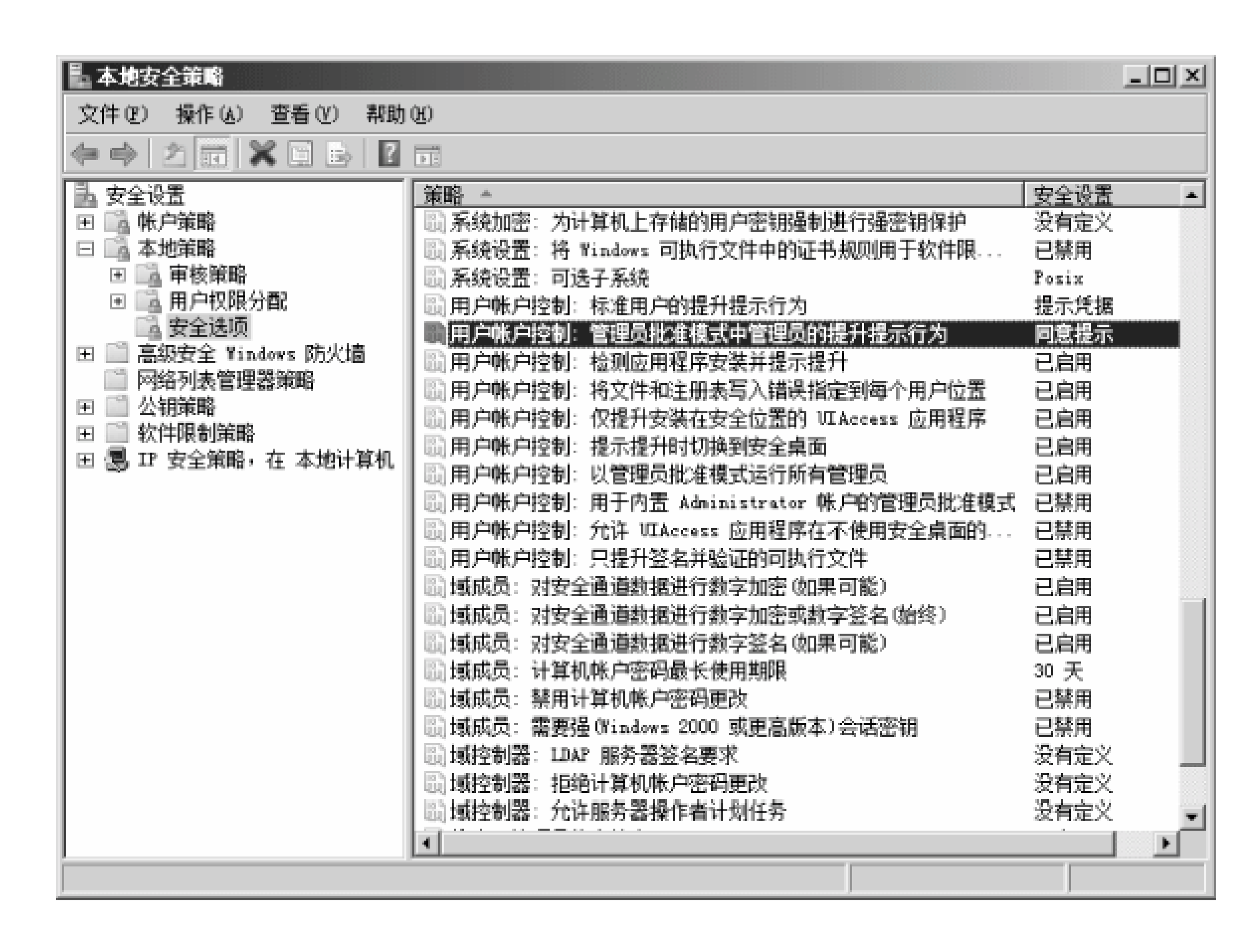


图 2-62 "本地安全策略"窗口

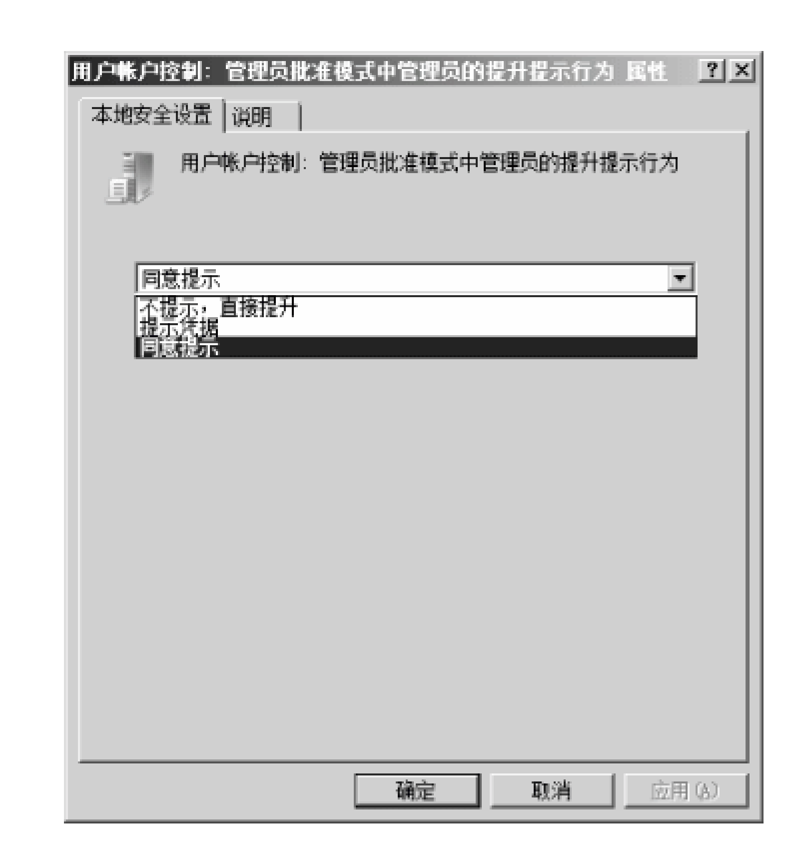


图 2-63 "用户账户控制：管理员批准模式中管理员的提升提示行为 属性"对话框

提示：该安全策略的提示行为包括以下几个选项。

① 同意提示。需要提升权限的操作将提示许可管理员选择允许或拒绝。如果许可管理员选择允许，则操作将使用可用的最高权限继续进行。此选项允许用户输入其姓名和密码来执行特权任务。

② 提示凭据。需要提升权限的操作将提示许可管理员输入其用户名和密码。如果用户输入有效凭据，则操作将使用适用权限继续进行。

③ 不提示，直接提升。此选项允许许可管理员执行需要无许可或凭据的提升的操作。需要注意的是，此方案仅用于大多数限制的环境中。

(3) 单击“确定”按钮，保存设置即可。同时，管理员可以使用该方法更改与“用户账户控制”功能相关的其他策略。

3. UAC 的应用类型

UAC 的主要功能是对本地系统用户账户操作进行控制和限制，例如用户运行系统管理程序、安装应用程序或修改系统设置的操作等。普通用户只需得到管理员账户的授权，就可以实现所需的管理操作。

应用程序尝试使用管理员的完全存取令牌运行时，Windows Vista 和 Windows Server 2008 会分析可执行文件以确定其发行者，并使用此信息来决定正确的用户体验。例如，在如图 2-64 所示的“用户账户控制”对话框中，提示信息背景颜色为灰色，表明需要管理权限的应用程序是通过代码验证签名的，且属于本地计算机的信任程序，如 Microsoft 防火墙客户端和 ISA(Internet Security and Acceleration Server)服务器。

在如图 2-65 所示的“用户账户控制”对话框中，提示信息背景颜色为黄色，表明需要管理权限的应用程序不具有正确代码验证签名，因此运行它是有一定风险的。



图 2-64 应用程序已由代码验证签名且受本地计算机信任



图 2-65 应用程序未经签名时的提示信息

在如图 2-66 所示的对话框中，提示信息背景颜色为红色，并且盾牌图标也变为“红底白叉号”，表明需要管理权限的应用程序来自被阻止或是非受信的发布者。管理员可以将发布者签名证书存放在本地计算机的非受信证书库中，以便阻止特定的发布者，当然，也可以使用组策略来达到同样的目的。

注意： UAC 对话框会根据发布者的代码验证签名信任级别，来决定其所显示的细节信息，包括可执行名称和路径。

通常情况下，“控制面板”窗口中的某些组件配置窗口中会显示 UAC 提示验证图标，如图 2-67 所示的“日期和时间”对话框。默认用户可以查看时钟和更改时区，而要更改本地系统时间，则需要完全管理员访问令牌。原因很简单，如果用户更改了系统时间，那么，将导致事件日志中的事件混乱，或者将影响计算机访问 Windows 域时的验证。

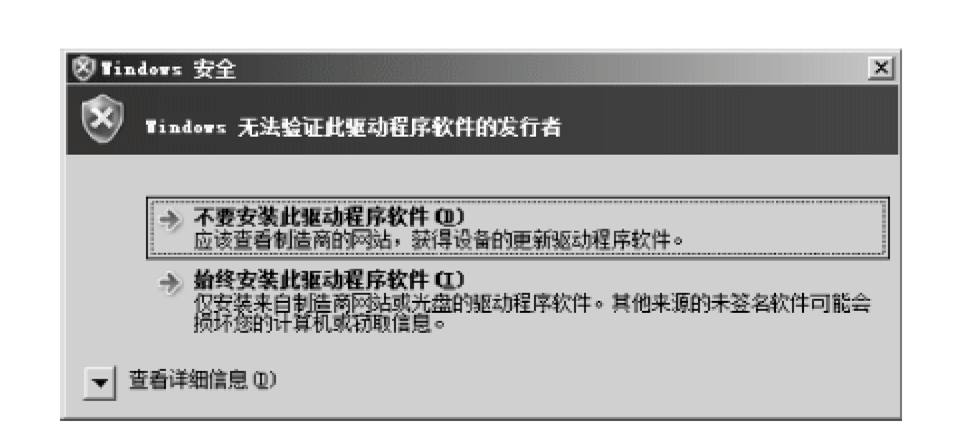


图 2-66　阻止特定的发布者



图 2-67　"日期和时间"对话框

2.3.8　知识链接：配置系统安全

1. Windows Update

Windows Update 的主要功能是获取并安装系统更新，弥补系统漏洞。Windows Server 2008 系统中，管理员无论是登录 Microsoft Update 网站，还是运行系统中的 Windows Update 组件都可以启动 Windows Update 向导。默认情况下，Windows Update 是未配置的，用户可以根据需要选择适当的下载和安装模式。

2. Administrator 账户安全

系统管理员账户是 Windows 系统中权限最高的用户账户，一旦被入侵者破解或丢失，后果将不堪设想。更改账户名称和创建陷阱账户是最常用最有效的方法。

安装 Windows Server 2008 系统后，默认会自动创建一个系统管理员账户，即 Administrator。因此，许多黑客攻击服务器时总是试图破解 Administrator 账户的密码，达到入侵的目的。通过更改管理员账户名称来避免此类攻击，提高系统安全性。

所谓陷阱账户就是名称与默认管理员账户名称(Administrator)类似或完全相同，而权限却极低的用户账户。这种方法通常和"更改 Administrator 账户名称"配合使用，即将系统管理员账户更名后，再创建一个名称为 Administrator 的陷阱账户。

3. Internet 防火墙

Windows Server 2008 的 ICF(Internet Connection Firewall，Internet 连接防火墙)是一种典型的状态防火墙，不仅可以监视通过其路径的所有通信，并且检查所处理的每一条消息的源地址和目的地址，工作方式如图 2-68 所示。

ICF 就像一个在计算机和外部 Internet 之间建立的"盾牌"，可以允许请求的数据包通过，而阻碍那些没有请求的数据包，因此它是一个动态数据包过滤器。它可以对直接连接 Internet 或连接在运行 ICF 的"Internet 连接共享主机"后的计算机提供保护。启用后，ICF 会禁止所有来自 Internet 的未经允许的连接。为此，防火墙使用"网

图 2-68　Internet 防火墙

络地址转换器(NAT)”逻辑来验证访问网络或本地主机的入站请求。如果网络通信不是来自受保护的网络内,或者没有创建任何端口映射,入站数据将被丢弃。

通常情况下,黑客入侵的第一步就是找到所要攻击主机的 IP 地址,再使用 ping 命令测试到该主机的连通性,然后对主机进行端口扫描,查看哪些端口是开放的,最后找出系统漏洞进行攻击。如果攻击个人计算机,通常是通过扫描一段 IP 地址开始来锁定目标,这种情况下,ping 不通的 IP 地址通常被认为没有使用而忽略过去。因此,ICF 的第一个功能就是不响应 ping 命令,而且,ICF 还禁止外部程序对本机进行端口扫描,抛弃所有没有请求的 IP 数据包。如此一来,可以被黑客利用的系统漏洞就很少了。

ICF 是通过保存一个表格,记录所有自本机发出的目的 IP 地址、端口、服务以及其他一些数据来达到保护本机的目的。当一个 IP 数据包进入本机时,ICF 会检查这个表格,看到达的这个 IP 数据包是不是本机所请求的,如果是就让它通过,如果在这个表格中没有找到相应的记录就抛弃这个 IP 数据包。

4. Windows 默认共享

默认共享是为了方便管理员远程管理而默认开启的共享,即所有的逻辑磁盘(C$、D$、E$ 等)和系统目录 Windows NT 或 Windows(ADMIN$),通过 IPC$ 连接可以实现对这些默认共享的访问。如果在网络中没有使用默认共享的必要,建议用户将系统的默认共享关闭,从而进一步地保证计算机的安全。

5. Windows 系统服务

(1) 服务账户

系统服务只有在特定账户登录的情况下才会运行,通常情况下无须更改服务的默认登录账户。如果选定账户没有登录计算机服务的权限,Microsoft 管理控制台(MMC)的服务管理单元将自动为该账户授予登录服务的用户权限,但并不一定会启动服务。服务的登录账户可以分为如下几种类型。

① 本地系统账户(LocalSystem)。使用该账户登录的服务,可以访问整个域。

② 本地服务账户(NTAUTHORITY\LocalService)。它是一种特殊的内置账户,类似于经过身份验证的用户账户。以“本地服务账户”运行的服务使用有匿名凭据的空会话来访问网络资源。

③ 网络服务账户(NTAUTHORITY\NetworkService)。与本地服务账户类似,但是“网络服务”账户运行的服务可使用计算机账户的凭据来访问网络资源。

注意:如果更改默认服务设置,重要的服务可能无法正常运行。最重要的是,更改启动类型一定要谨慎,要使用配置了自动启动服务的设置来登录。

(2) 漏洞和应对措施

通常情况下,为服务设置适当的启动方式,是避免服务漏洞攻击的首选方式。Windows Server 2008 系统服务提供如下 4 种启动方式。

① 自动。此服务随着系统启动时启动。

② 手动。用户根据需要以手动方式启动或禁用服务,以节省系统资源。

③ 已禁用。此类服务不能再运行。

④ 自动(延迟的启动)。延缓服务的启动,以减小系统载入时的负荷。

对于所有非必要的服务应当禁用。除此之外,还可通过配置用户定义账户列表的访问

控制列表(ACL)来编辑服务安全性。

(3) 服务权限

每个服务都有特定的权限,管理员可以将这些权限授予每一个用户或组,也可以从用户或组的权限中取消相应的服务权限。服务具有的权限及描述如表 2-1 所示。

表 2-1 服务权限

权　限	描　述
完全控制	执行所有功能。默认情况下,服务会自动授予登录用户完全控制权限
查询模板	确定与某个服务对象关联的配置参数
更改模板	更改服务的配置,如更改启动类型
状态查询	有关服务状态的访问信息
列举依存关系	确定依存于指定服务的所有其他服务
启动	启动服务
停止	停止服务
暂停和继续	暂停或继续服务
询问	报告服务的当前状态信息
用户定义的控制	将用户定义的控制请求或特定于服务的请求发送给该服务
删除	删除服务
读取权限	读取指派给服务的安全权限
更改权限	更改指派给服务的安全权限
取得所有权	更改安全密钥,或更改关于不为用户所有的服务的权限

6. 用户账户控制

用户账户控制(User Account Control,UAC)是 Microsoft 为提高系统安全而在 Windows Vista 中引入的新技术,它允许用户验证系统行为,从而阻止未经认证的计算机系统的变动。当用户以管理员身份登录到 Windows Vista 和 Windows Server 2008 时,会得到两个访问令牌:一是完全访问令牌;二是标准受限访问令牌。

标准受限访问令牌对受限进程没有管理特权,并且禁用管理员组安全标识符(Security Identifier,SID),主要用于启动 Windows 资源管理器和所有的子进程。所有应用程序默认都是以标准受限访问令牌运行的,除非管理员授予其权限,否则不能以完全访问令牌运行。注意,由于应用程序将继承父进程的特权级别,因此,如果父进程以完全访问令牌运行,则子进程也会继承其特权级别,且不会提示管理员。例如,以管理员身份运行命令提示符,则在命令提示符下运行的所有进程都将具备管理员特权。

提示:Explorer.exe 默认是非提升权限的,所以,当右击选择"以管理员身份运行"选项时,会重新启动一个与原窗口同样的窗口。管理员可以借助相关工具,在每个文件夹的右键快捷菜单中添加一个 Elevate Explorer Here 命令。这样,就可以随时随地启动一个提升了权限的 Windows Explorer 了。Explorer.exe 进程并不是系统运行时所必需的,所以,可以用任务管理器来结束它,并不影响系统的正常工作。

2.4 系统漏洞扫描

漏洞扫描是网络安全防御中的一项重要技术，其原理是采用模拟攻击的形式对目标可能存在的安全漏洞进行逐项检查，其目标是工作站、服务器、数据库应用程序等。根据扫描结果向系统管理员提供周密可靠的安全性评估分析报告，从而为提高网络安全整体水平产生重要依据。MBSA 是 Microsoft 免费推出的系统漏洞扫描产品，支持的系统平台包括 Windows NT/2000/XP/2003/2008，支持类型涵盖了微软公司的大部分产品。

2.4.1 使用 MBSA 扫描本地系统漏洞

使用 MBSA 扫描本地系统漏洞的具体步骤如下。

(1) 依次选择"开始"→"所有程序"→Microsoft Baseline Security Analyzer 2.1 选项，打开如图 2-69 所示的 MBSA 主窗口。



图 2-69 MBSA 主窗口

(2) 单击 Scan a computer 链接，显示如图 2-70 所示的 Which computer do you want to scan 窗口。在 Computer name 文本框中，指定要扫描的计算机名，系统默认为本地计算机。用户可以根据需要，选择此次扫描的目标服务或应用程序，如 IIS、SQL、密码安全性等，这里只选择前两项扫描功能。

提示：在 Security report name 文本框中显示的是系统默认的扫描结果名称格式，其中"%D%"表示域名称，"%C%"表示目标计算机名称，"(%T%)"表示扫描日期和时间，如果是基于 IP 地址的扫描任务，则还会出现"%IP%"，表示被扫描主机的 IP 地址。

(3) 根据需要选择需要检测的安全内容。然后单击窗口下方的 Start Scan(开始扫描)按钮，系统开始进行扫描。完成后显示如图 2-71 所示的扫描结果窗口。在 Potential Risk (潜在风险)选项区域显示了被扫描主机的基本信息，包括主机名、IP 地址和扫描日期等；在 Windows Scan Results(Windows 扫描结果)选项区域显示了扫描结果摘要信息。管理员通过每项扫描结果前不同的图标，即可判断其安全状态。

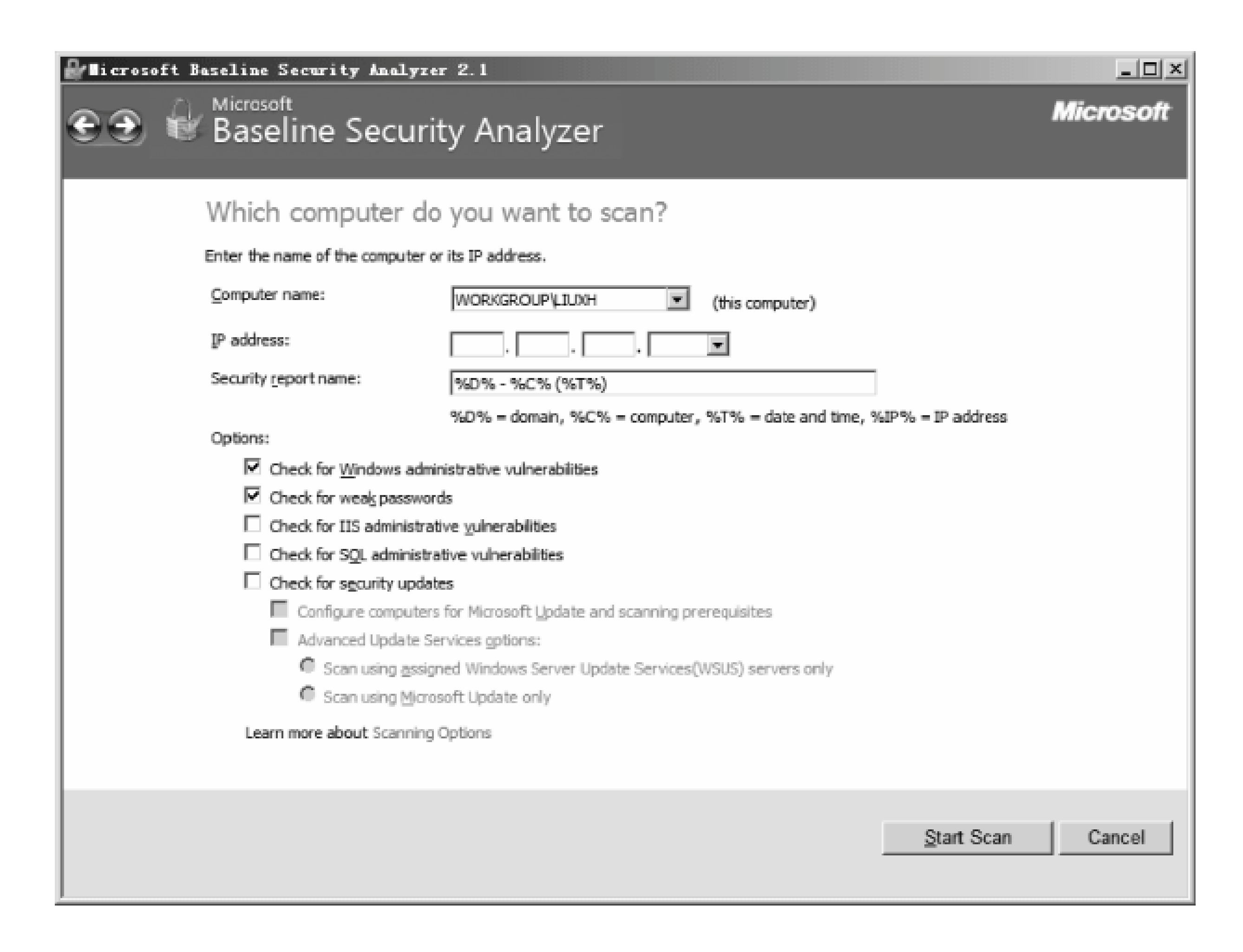


图 2-70 Which computer do you want to scan 窗口

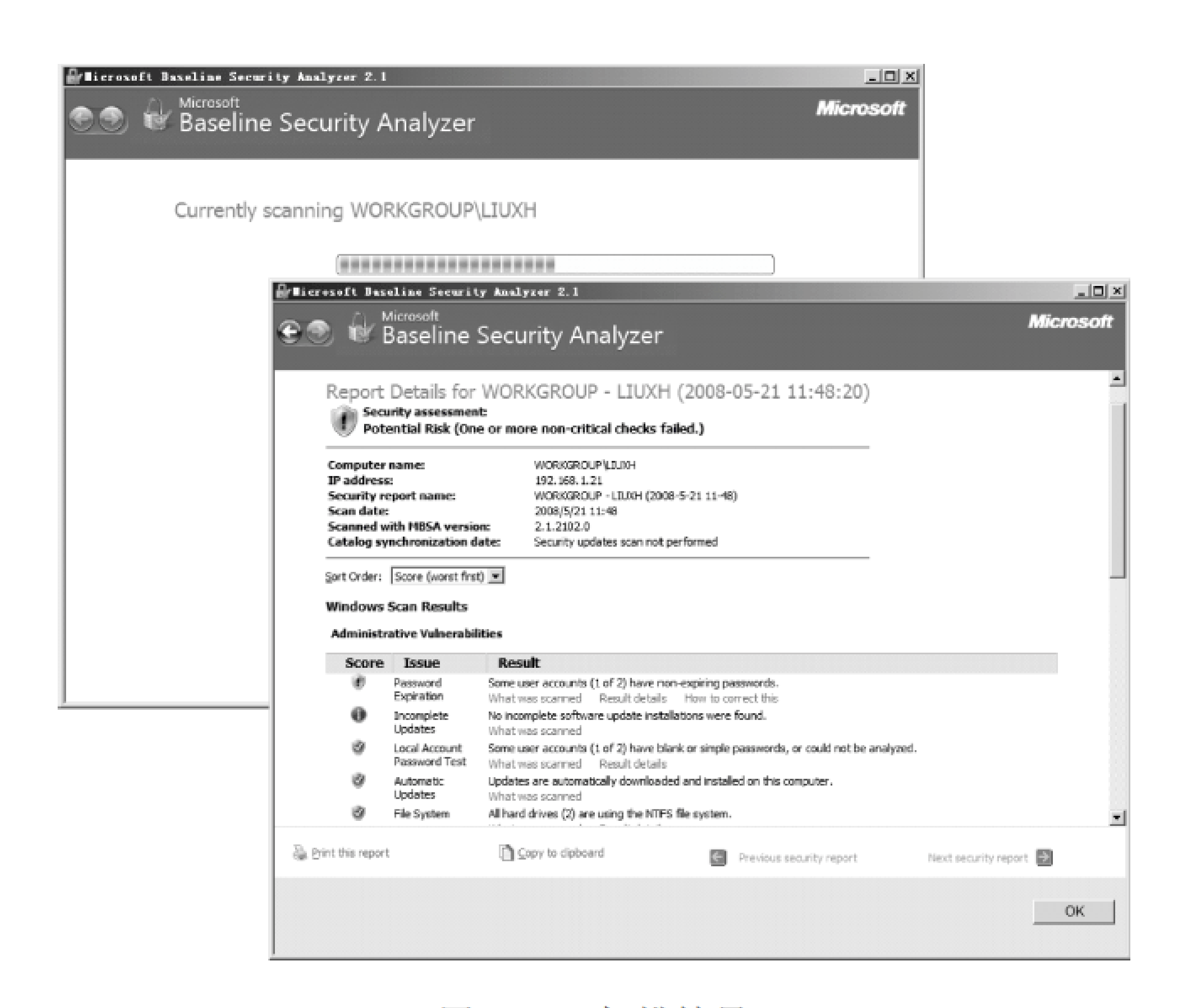


图 2-71 扫描结果

(4) 在 Issue(问题)栏中列出了被扫描计算机存在的主要安全问题,这里以扫描结果中的 Password Expiration(密码过期)问题为例。单击 What was scanned(扫描对象)链接,打开如图 2-72 所示的 Password Expiration 窗口,信息中提示该项检查将列出目标计算机系统中,所有密码过期或不符合要求的账户。

(5) 在扫描结果窗口中,单击 Result details(详细结果)链接,打开如图 2-73 所示的 Result Details 窗口,提示目标计算机的 Guest 账户密码已经过期。

(6) 在扫描结果窗口中,单击 How to correct this(如何改正错误)链接,打开如图 2-74 所示的窗口。其中,在 Solution(解答)部分将给出合理的解决方法;在 Instructions(操作步骤)部分根据被扫描计算机系统类型,给出详细的操作流程。

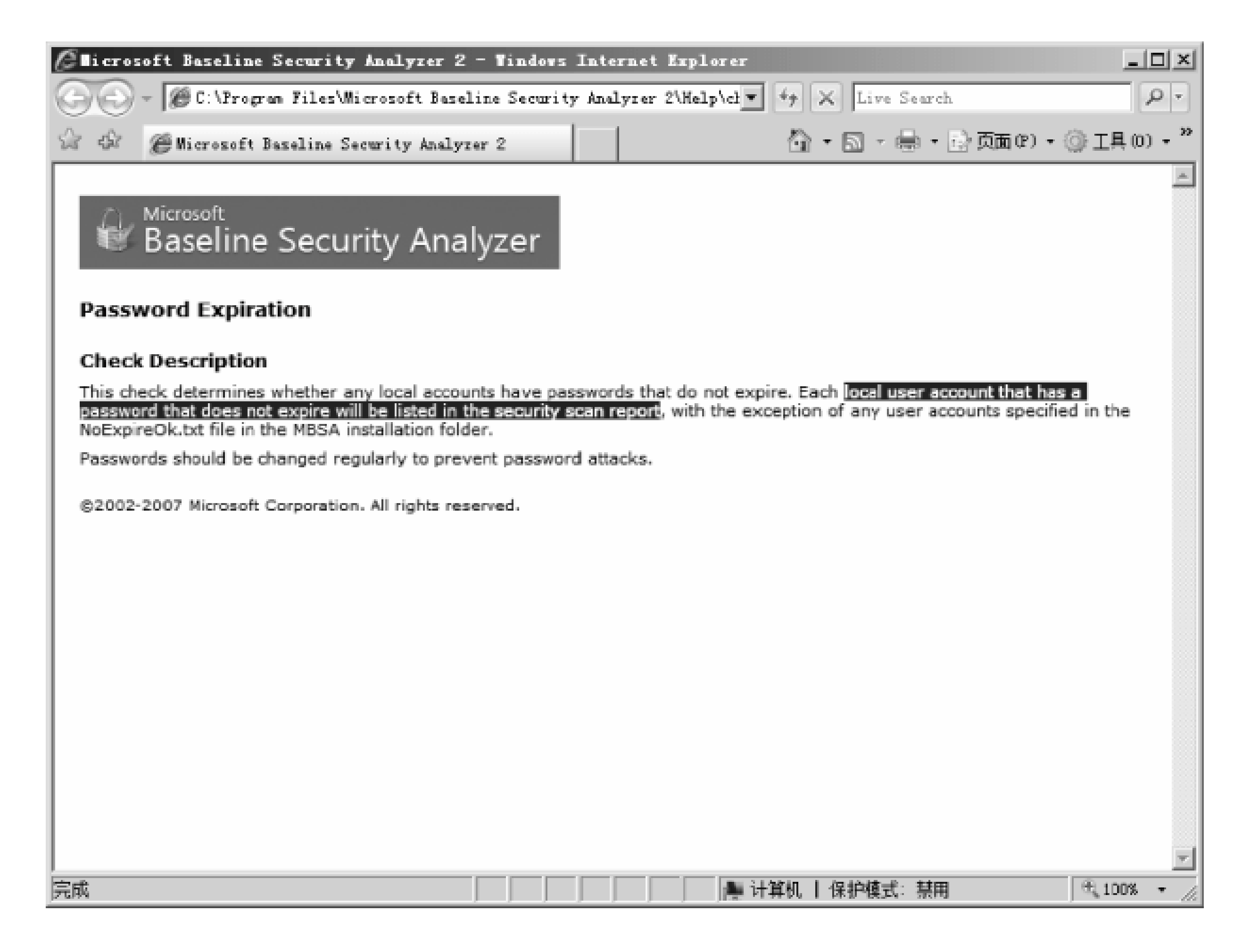


图 2-72　Password Expiration 窗口

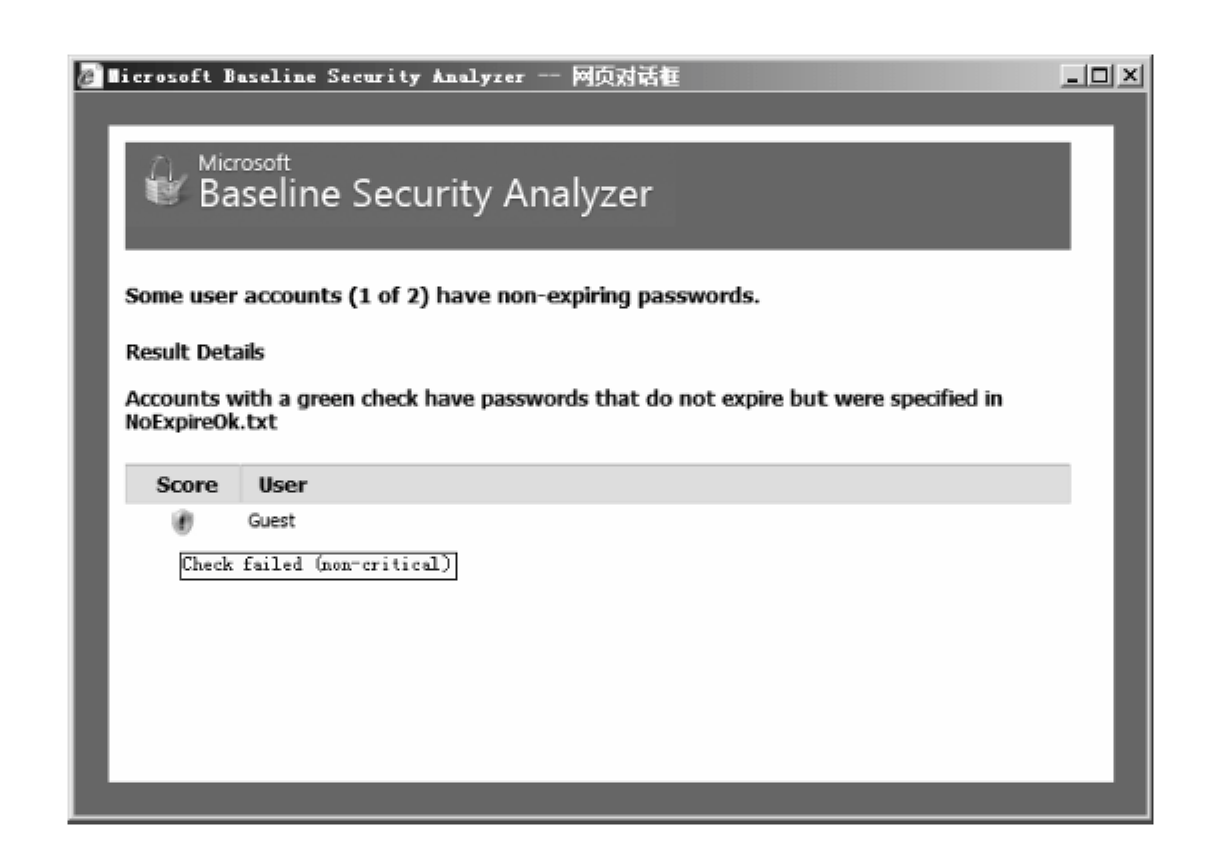


图 2-73　Result Details 窗口

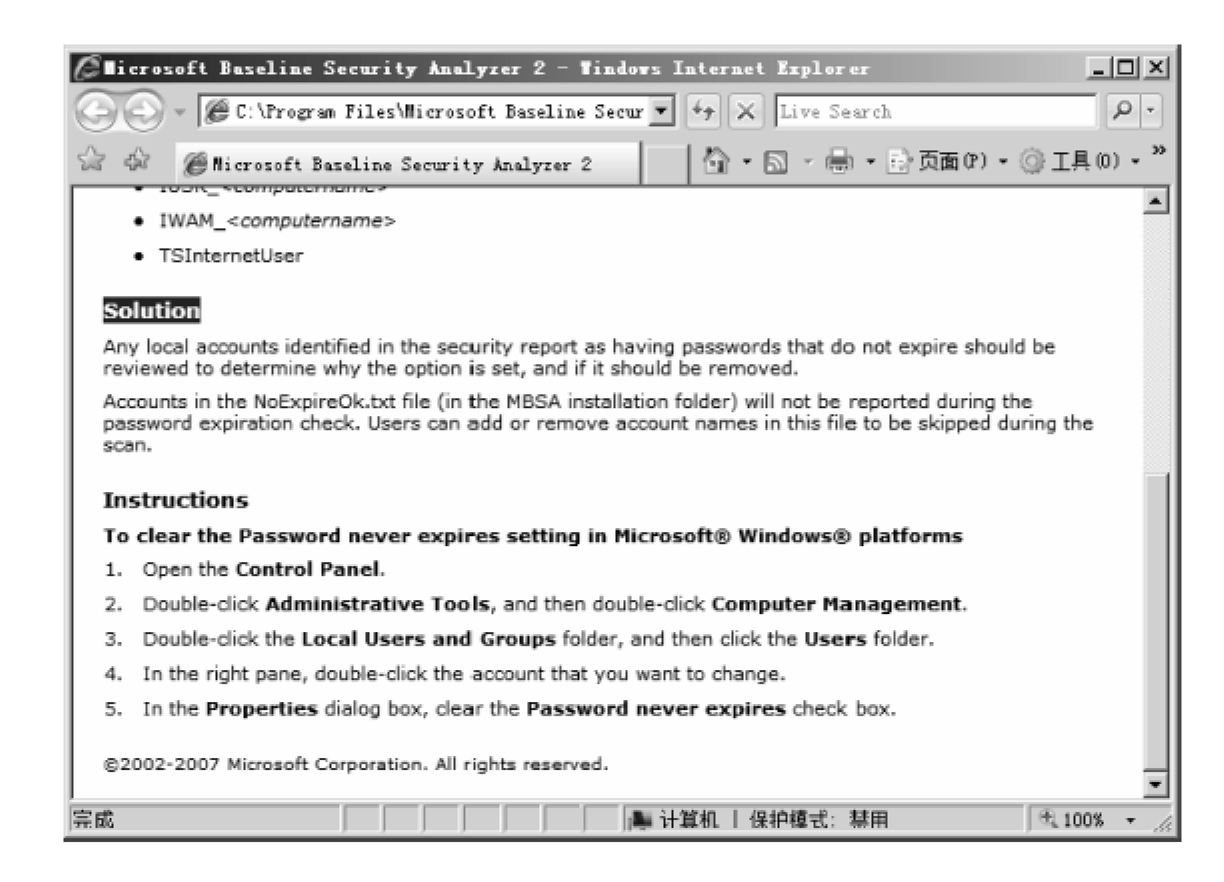


图 2-74　解决方法

提示：对于 Check passed(通过检查)的扫描结果，则不会出现 How to correct this 链接。

(7) 在扫描结果窗口中，单击 OK 按钮结束此次扫描。

2.4.2 扫描单台远程计算机

使用 MBSA 扫描远程主机 Windows 漏洞，比扫描本地计算机要复杂一些，并且 Windows 域环境和工作组环境中的操作也有所不同。由于 MBSA 的工作机制是基于用户账户的，所以扫描远程计算机时，必须拥有远程计算机中相关权限的用户账户。在 Windows 域环境中，使用域管理员账户即可，如果是扫描工作组中的远程计算机，则开始之前必须做好如下准备工作。

(1) 在运行 MBSA 的计算机上，以 Administrator 账户或 Administrators 组中的成员登录系统。

(2) 在目标计算机上同样以 Administrator 账户或 Administrators 组中的成员登录系统，并开启 Guest 账户。

(3) 将 Guest 账户添加到 Administrators 组中。

(4) 修改目标计算机组策略，使 Guest 账户拥有远程访问权限。

以扫描操作系统为 Windows XP 的远程计算机为例，主要操作步骤如下。

(1) 在目标计算机上，展开“计算机管理”窗口中的“本地用户和组”→“用户”选项，双击 Guest 账户打开“Guest 属性”对话框。默认情况下，Guest 账户是被禁用的，取消“账户已停用”复选框即可，如图 2-75 所示。

(2) 切换至“隶属于”选项卡，单击“添加”按钮打开“选择组”对话框，在“输入对象名称来选择(示例)”文本框中输入 Administrators，如图 2-76 所示。也可以单击“高级”按钮在所有本地用户组中查找。最后单击“确定”按钮，将其添加到 Guest 账户隶属的组中。

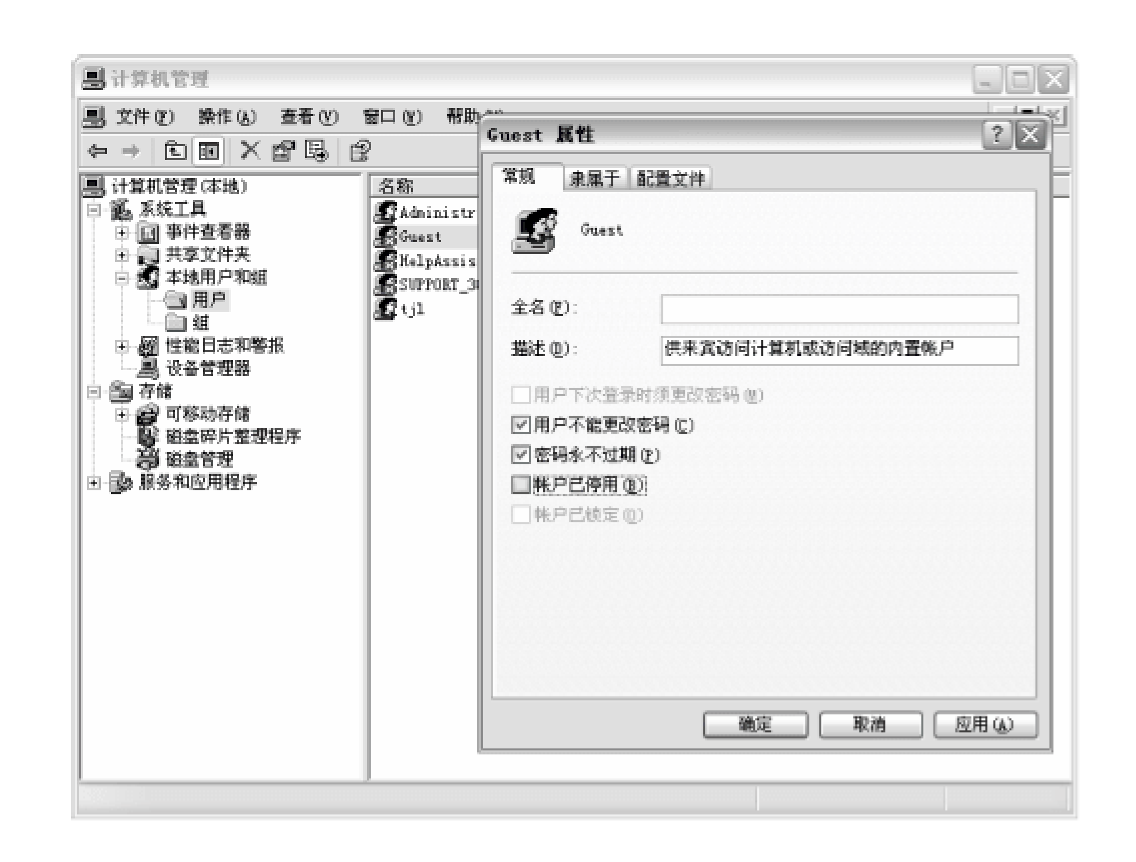




图 2-75 启用 Guest 账户

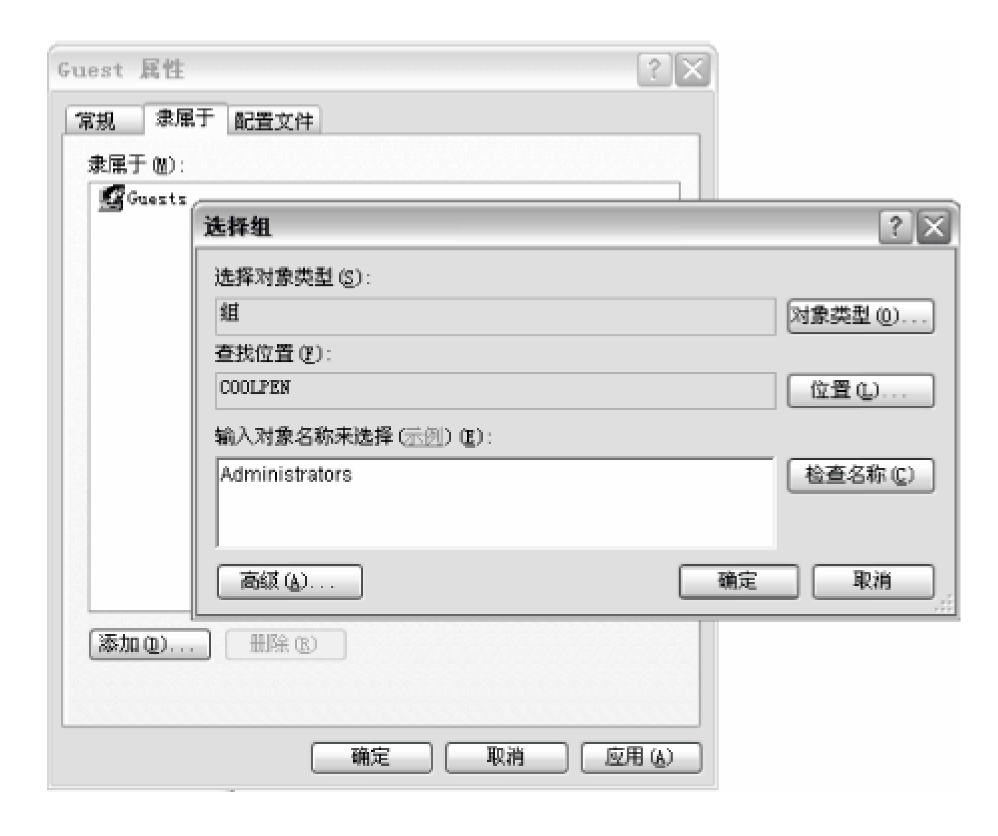


图 2-76 将 Guest 账户添加至 Administrators 组

提示：将 Guest 账户添加至 Administrators 组中的操作是非常危险的，建议远程扫描完毕后立即将其从 Administrators 组中删除，并再次禁用。

(3) 打开“组策略”窗口，并依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”选项，如图 2-77 所示。主要设置“从网络访问此计算机”和“拒绝从网络访问这台计算机”策略。



图 2-77 “组策略”窗口

（4）双击“从网络访问此计算机”，打开“从网络访问此计算机 属性”对话框，默认状态下 Guest 账户是不在其中的，单击“添加用户或组”按钮，打开“选择用户或组”对话框，在“输入对象名称来选择(示例)”文本框中输入 Guest，如图 2-78 所示。

（5）单击“确定”按钮，将其添加至允许远程访问的用户和组列表中。单击“应用”或“确定”按钮，显示如图 2-79 所示的“确认设置更改”对话框，提示此设置可能导致的系统问题，单击“是”按钮继续即可。



图 2-78 允许 Guest 账户从网络访问此计算机

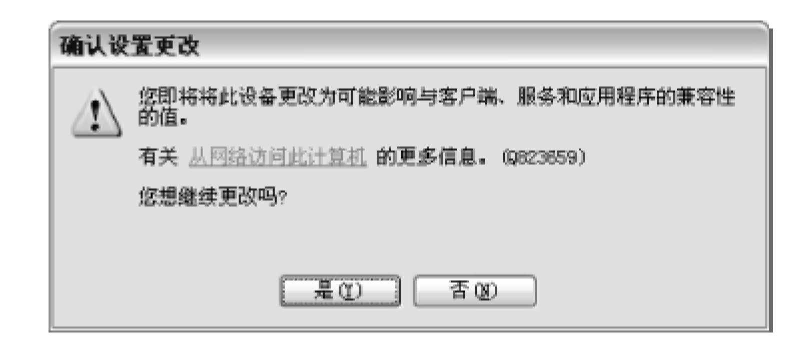


图 2-79 “确认设置更改”对话框

（6）在“组策略”窗口中，双击“拒绝从网络访问这台计算机”，打开“拒绝从网络访问这台计算机 属性”对话框，显示如图 2-80 所示，选择 Guest 账户并单击“删除”按钮，将其从拒绝远程访问的用户账户列表中删除即可。最后，单击“确定”按钮保存设置。

（7）在执行远程扫描任务的计算机上打开 MBSA，单击 Scan a computer 链接，打开 Which computer do you want to scan 窗口。在 Computer name 文本框中按照“工作组名\计算机名”的格式输入被扫描计算机的相关信息，也可以通过 IP 地址指定，如图 2-81 所示。

（8）单击 Start Scan 按钮即可开始扫描，扫描结果与扫描本地计算机类似，如图 2-82 所示，此处不再赘述。



图 2-80　删除"拒绝从网络访问这台计算机"列表中的 Guest 账户

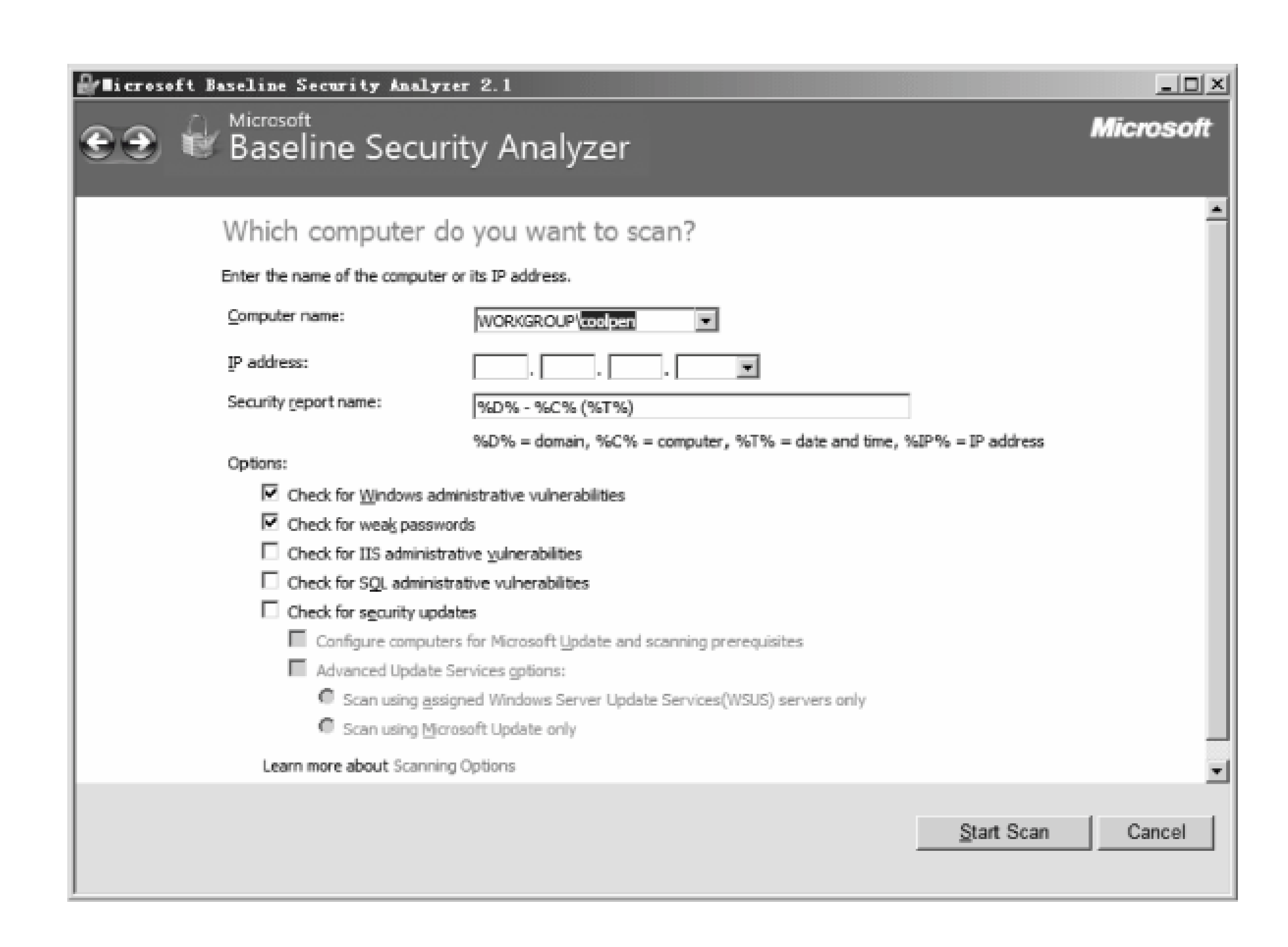


图 2-81　扫描单台远程计算机

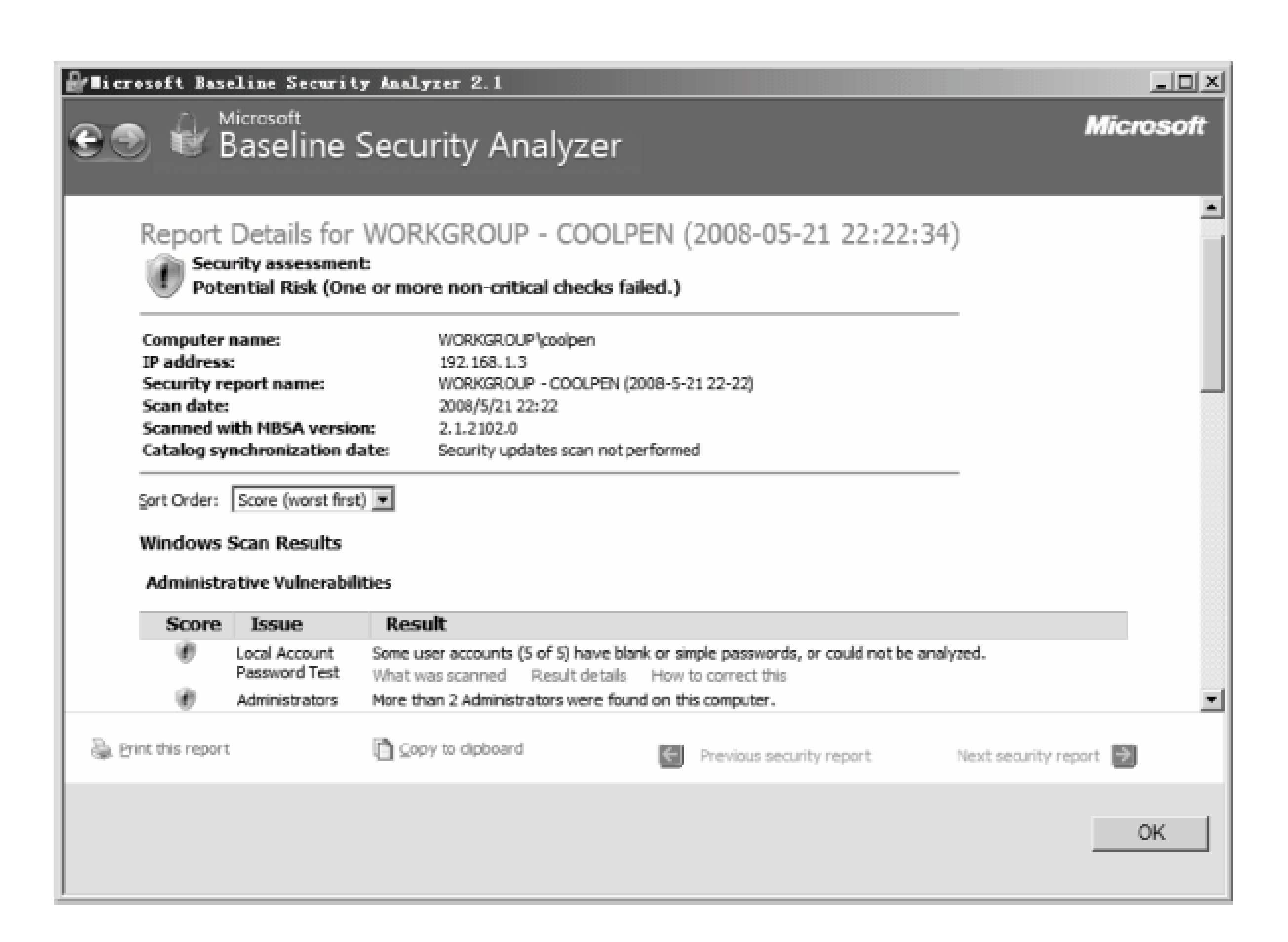


图 2-82　远程计算机扫描结果

提示：如果准备工作不充分，则可能会导致无法扫描到远程主机，常见错误提示信息包括如下几种。

(1) User is not an administrator on the scanned machine：被扫描计算机上开放的远程访问用户不是系统管理员，或没有被添加到管理员组中。

(2) This is not a Windows NT/2000/XP/2003 Server or Workstation：被扫描计算机不是 Windows NT 4.0/2000/XP/2003 系统，因为 MBSA 不支持对 Windows 9x 系统的 Windows 系统漏洞扫描。

(3) The operating system returned error message 1385 登录失败：未授予用户在此计算机上的请求登录类型：被扫描计算机上开放的账户未被赋予远程访问权限。

2.4.3　知识链接：MBSA

MBSA 全称 Microsoft Baseline Security Analyzer，此工具允许用户扫描一台或多台基

于 Windows 系统的计算机，以及发现常见安全方面的配置错误，并检查操作系统和已安装的其他组件，及时通过推荐的安全更新进行修补。MBSA 的免费下载地址为：http://www.microsoft.com/downloads/details.aspx?FamilyID=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en。

1. 扫描模式

MBSA 允许扫描一台或者多台计算机。

(1) 单台计算机。MBSA 最简单的运行模式是扫描单台计算机。默认情况下，将扫描本地计算机，管理员也可以通过指定计算机名或 IP 地址方式，使其扫描其他计算机。扫描远程计算机时，当前用户账户必须拥有目标计算机的远程访问权限。

(2) 多台计算机。如果选择"选取多台计算机进行扫描"时，可以选择通过输入域名扫描整个域，或指定一个 IP 地址范围并扫描该范围内的所有基于 Windows 系统的计算机。

注意：扫描远程单台主机或其他网段的计算机，必须使用具有相关权限的用户账户。在进行"自动扫描"时，用来运行 MBSA 的账户也必须是管理员或者是本地管理员组的成员。

2. 扫描类型

MBSA 支持两种类型的扫描模式。

(1) MBSA 典型扫描。MBSA 典型扫描将执行扫描并且将结果保存在单独的 XML 文件中，这样就可以在 MBSA 查看器中进行查看。可以通过 MBSA GUI 方式(mbsa.exe)或 MBSA 命令行方式(mbsacli.exe)进行 MBSA 典型扫描，扫描内容包括所有可用的 Windows、IIS、SQL 和安全更新检查。每次执行 MBSA 典型扫描时，都会为每一台接受扫描的计算机生成一个安全报告，并保存在正在运行 MBSA 的计算机中。

(2) HFNetChk 典型扫描。HFNetChk 典型扫描将只检查缺少的安全更新，并以文本的形式将扫描结果显示在命令行窗口中。与以前独立版本的 HFNetChk 处理方法完全相同。这种类型的扫描可以通过带有"/xmlout"开关参数(指示 MBSA 工具引擎进行 HFNetChk 扫描)的 mbsacli.exe 来执行。

3. 网络扫描

MBSA 最多可以允许从服务器同时对 10000 台计算机进行远程漏洞扫描。在防火墙或路由器将两个网络分开的多域环境中(两个单独的 Active Directory 域)，TCP 的 139 端口和 445 端口以及 UDP 的 137 端口和 138 端口必须开放，以便 MBSA 连接和验证所要扫描的远程网络主机。

4. 操作系统检查

MBSA 对被扫描的计算机中的 Windows 操作系统进行扫描，表 2-2 所示列出了扫描过程中检测的项目。

5. 安全更新检查

MBSA 对在被扫描的计算机中的安全更新列表进行扫描，并检测是否存在由于安装更新补丁产生的新漏洞。该项检查将确保具有针对下列产品和组件的最新服务包和安全更新。

表 2-2 MBSA 的扫描项目

检测项目	描述
Administrators 成员权限	确定并列出属于本地管理员组的用户账户。如果检测出的单个管理员账户数量超过两个,则该工具将列出这些账户名,并将该检查标记为一个潜在的安全漏洞
审核	确定在被扫描的计算机上是否启用了系统审核功能。Windows 系统的审核特性,可跟踪和记录系统上的特定事件,如成功的和失败的登录尝试。通过监视系统的事件日志,可以发现潜在的安全问题和恶意活动
自动登录	确定在被扫描的计算机上是否启用了"自动登录"功能,以及登录密码是否在注册表中以密文方式存储。如果"自动登录"已启用而且密码以加密形式存储在注册表中,那么安全报表就会将这种情况作为一个潜在的安全漏洞标记出来。默认情况下,Windows Server 2008 禁止"自动登录"
自动更新	确定是否在被扫描的计算机上启用自动更新功能,以及详细的配置情况。当用户使用直接下载更新方式之外的其他方式时,扫描结果中可能会出现相关安全警告信息,提示自动更新没有正确配置,此时不必理会
域控制器	确定正在接受扫描的计算机是否为域控制器,这主要是针对 Windows Server 2003 和 Windows Server 2008 系统而言的。如果是域控制器,则同时检测是否采取了相应的操作来加强访问安全
文件系统	确定在每个分区使用的文件系统类型。NTFS 具有访问控制功能,是一个安全的文件系统,因此,服务器所有分区均使用该文件系统,如果使用 FAT32 文件系统,则扫描结果中将报警
Guest 账户	确定在被扫描的计算机上是否启用了系统内置的 Guest 账户。来宾账户主要视为临时用户提供的,默认情况下是禁用的。如果在 Windows NT/2000/XP/2003/Vista/2008 计算机上已启用来宾账户,则此时将在安全报表中作为一个安全漏洞标记出来
Windows 防火墙	确定是否在被扫描的计算机上对所有的活动网络连接启用 Windows 防火墙,这主要是针对 Windows XP/2003/2008 系统而言的。如果已经启用防火墙,则还将对其开放的入站端口进行检测。如果 Windows 防火墙没有开启,或者开放了存在安全漏洞的端口,则扫描结果中将出现警告信息
本地账户密码	确定被扫描计算机的本地用户账户密码是否为空或者简单密码。在 Windows Server 2008 系统中,必须设置符合相应复杂程度的安全密码,才允许启用管理员账户
密码过期	确定是否有本地用户账户设置了永不过期的密码。密码应该定期更改,以降低遭到密码攻击的可能性
限制匿名用户	确定被扫描的计算机上是否使用了 RestrictAnonymous 注册表项来限制匿名连接
共享资源	确定在被扫描的计算机上是否存在共享文件夹。扫描报告将列出在计算机上发现的所有共享内容,其中包括管理共享及其共享级别和 NTFS 级别的权限。扫描结果中将列出所有的系统默认共享,和用户后期设置的重要资源共享
检查是否存在不必要的服务	确定被扫描计算机上的 services.txt 文件的服务列表中,是否包含有已启用的非必要服务。services.txt 随 MBSA 的安装自动生成,并且是可配置的,默认情况下包括 MSFTPSVC(FTP)、TlntSvr(Telnet)、W3SVC(WWW)和 SMTPSVC(SMTP)。如果被扫描计算机上安装了列表中指定的服务,则扫描结果中将出现警告

(1) Windows NT 4.0(除非通过 mbsacli.exe /xmlout 进行扫描,否则只能进行远程扫描)。

(2) Windows 2000/XP/ Vista。

(3) Windows Server 2003/2008。

(4) Internet Explorer 5.01 和后续版本。

(5) Windows Media Player 6.4 和后续版本。

(6) IIS 4.0 和后续版本。

(7) SQL Server 7.0/2000/2005(包括 Microsoft Data Engine)。

(8) Exchange Server 5.5/2000/2003/2007(包括 Exchange Admin Tools)。
(9) Microsoft Office(只能进行本地扫描)。
(10) Microsoft Data Access Components(MDAC)2.5/2.6/2.7/2.8。
(11) Microsoft Virtual Machine。
(12) MSXML 2.5/2.6/3.0/4.0/5.0/6.0。
(13) BizTalk Server 2000/2002/2004/2006。
(14) Commerce Server 2000/2002。
(15) Microsoft Content Management Server(MCMS)2001/2002。
(16) SNA Server 4.0、Host Integration Server(HIS)2000 和 2004。

2.5 端口安全

端口,是服务器上的网络服务得以对外提供的主要通道,一台被配置 IP 地址的服务器,可以提供多种不同的网络服务,这主要是因为每个网络服务使用的端口是不同的。每个 IP 地址可提供 65536 个端口,有些端口是默认开放的,有些则是关闭的,而开放的端口随时都有可能成为非法入侵者的跳板,因此,必须充分了解计算机的端口开放情况。

2.5.1 查看端口开放情况

查看当前有哪些计算机正在与本机连接,以及所使用的 IP 地址及端口等信息,如果想要达到这个目的,可以使用 netstat 命令行的方法。

单击"开始"按钮,在"开始搜索"文本框中,输入 cmd 并按 Enter 键,显示命令提示符窗口。在命令提示符下输入如下命令:

```
netstat -na
```

按 Enter 键执行命令,显示如图 2-83 所示结果。

```
管理员: 命令提示符

C:\Users\Administrator>netstat -na

活动连接

  协议  本地地址              外部地址            状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    211.82.218.225:139     0.0.0.0:0              LISTENING
  TCP    211.82.218.225:49166   211.82.218.229:445     ESTABLISHED
  TCP    211.82.218.225:49174   65.55.239.164:80       TIME_WAIT
  TCP    211.82.218.225:49194   221.195.3.41:80        ESTABLISHED
  TCP    211.82.218.225:49206   218.61.39.104:80       ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
```

图 2-83 查看当前端口连接

命令执行结果显示本机连接情况及打开的端口。其中包括"协议"、"本地地址"、"外部地址"和"状态"信息。"协议"表示通信协议的类型(TCP 或 UDP)。"本地地址"表示本地计算机的 IP 地址和正在使用的端口号。如果不指定-n 参数,则显示与 IP 地址和端口的名

称对应的本地计算机名称。如果端口还没有建立,那么端口将以星号(*)显示。“外部地址”表示连接该端口的远程计算机的 IP 地址和端口号。如果不指定-n 参数,则显示与 IP 地址和端口对应的名称。如果端口还没有建立,那么端口将以星号(*)显示。“状态”表示已建立连接的状态,通常包括 CLOSE_WAIT、CLOSED、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2、LAST_ACK、LISTENING、SYN_RECEIVED、SYN_SEND 和 TIME_WAIT 几种类型。

2.5.2 查看开放端口的宿主

所谓连接的宿主是指网络连接对应的应用程序或服务。通常情况下,仅凭开放端口是很难确认其安全与否的,发现可疑端口之后,首先要做的就是确认使用这些已经打开的端口的应用程序是哪个,然后进一步确认该程序是否为系统程序,如果不能确认,则可能是木马或其他非法程序。

在命令提示符窗口中输入如下命令:

```
netstat -bn
```

按 Enter 键执行命令,显示如图 2-84 所示结果。



图 2-84 显示应用程序打开的端口

在命令执行结果中,显示了当前活动的每个连接都是由哪些程序创建的,本例中端口 49400、49405、49407 和 49414 都是由 iexplore.exe 程序打开的,均被用于访问外网的 Web 服务器。如果在结果中发现计算机打开了可疑的端口,就可以使用该命令查看它调用了哪些组件,然后再检查各组件的创建时间和修改时间,如果发现异常,就可能是中了木马。

2.5.3 知识链接:端口划分与 netstat 命令

1. 端口划分

IP 地址的端口都是以端口号来标记的,端口号是 0~65535 的一个任意整数。按照端口号划分,可以将端口分为 3 大类,即公认端口、注册端口、动态或私有端口。

(1) 公认端口的范围为 0~1023。这些端口号一般被系统固定的分配给一些服务。

(2) 注册端口的范围为 1024~49511。注册端口松散绑定于一些服务,即端口号一般都不会固定地分配给某个服务,许多服务都可以使用这些端口。

(3) 动态或私有端口的范围为 49512～65535。通常情况下，不建议为服务分配这些端口。

端口按协议类型划分，可以分为 TCP、UDP 等端口。

(1) TCP 端口是由 TCP 协议而来的，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。

(2) UDP 端口，即用户数据包协议端口，无须在客户端和服务器之间建立连接，安全性得不到保障。

2. netstat 命令

netstat 主要用于显示活动的网络连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议)等。如果不使用任何参数，则显示系统内的活动的 TCP 连接。

netstat 命令的语法格式：

```
netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]
```

netstat 参数说明如下。

(1) -a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。

(2) -b：显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下显示包含于创建连接或监听端口的组件序列。这种情况下，可执行组件名在底部的[ ]中，顶部是其调用的组件。注意此选项可能需要很长时间，如果没有足够权限可能失败。

(3) -e：显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与-s 结合使用。

(4) -f：显示外部地址的完全限定域名(FQDN)。

(5) -n：显示活动的 TCP 连接，但只以数字形式表现地址和端口号，而不会确定其名称。

(6) -o：显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。可以在 Windows 任务管理器中的“进程”选项卡上，找到基于 PID 的应用程序。该参数可以与-a、-n 和-p 结合使用。

(7) -p proto：显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。如果该参数与-s 一起使用，按协议显示统计信息，则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6。

(8) -r：显示 IP 路由表的内容。该参数与 route print 命令等价。

(9) -s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果系统还安装了 Windows XP 的 IPv6 协议，就会显示有关 IPv6 上的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 协议的统计信息。可以使用-p 参数指定协议集。

(10) -t：显示当前连接卸载状态。

(11) interval：每隔一定时间重新显示一次选定的信息，单位是秒。按 Ctrl+C 键停止并重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息。

注意：与该命令一起使用的参数必须以连字符(-)作为前缀，而不能是短斜线(/)作为前缀。

习题

1. 简述 Windows Server 2008 系统的基本安全配置。
2. 如何为 Windows 系统设置安全密码？
3. 什么是端口？如何查看本地计算机端口开放情况？
4. 如何确保系统管理员账户的安全？

实验：扫描本地系统漏洞

实验目的：

掌握 MBSA 的基本应用。

实验内容：

运用 MBSA 扫描本地计算机存在的系统漏洞和应用程序漏洞。

实验步骤：

(1) 下载并安装 MBSA。

(2) 扫描本地系统漏洞。

(3) 查看扫描结果，找出系统漏洞对应的解决方案。

(4) 按照 MBSA 推荐的解决方案更改系统配置或安装补丁更新。

(5) 再次启动 MBSA 扫描系统，检查配置是否生效。

第 3 章 chapter 3

网络服务安全

网络应用服务安全是网络安全的一个重要方面,一旦出现安全问题轻则导致用户无法完成正常应用,重则导致重要数据丢失,后果非常严重。企业网络中常用的服务包括活动目录服务、文件服务和基于 IIS 的 Web 服务和 FTP 服务。基于 Windows Server 2008 系统的应用服务已经提供多项安全设置,用户只需根据需要合理配置即可。

3.1 网络服务安全规划

为客户端提供应用服务是计算机网络的主要功能,根据企业类型和实际需求的不同,需要部署的网络服务也会有所不同。网络服务安全是实现网络安全的重要环节,主要是解决网络服务源头的安全性和可靠性。

3.1.1 案例情景

该中型企业的网络规模并不大,运行的网络服务主要包括活动目录服务、文件服务、IIS 服务等。活动目录服务主要用于统一管理所有网络资源,为所有客户端访问提供身份验证,加强网络安全性。文件服务的主要功能是为客户端提供文件共享和存储服务,客户端使用域用户账户登录到域即可访问文件服务器的共享资源。网络中的 Web 服务和 FTP 服务都是基于 IIS 服务的,企业网站和内部办公网站均由 Web 服务器承载。

3.1.2 项目需求

在该企业的网络中,网络中心统一管理本地网络资源以及所有远程分支网络资源。分支机构的用户通过 VPN 远程拨叫到企业网络,访问网络内部共享资源。分支机构和企业网络之间的带宽也非常有限,对于分支机构的用户而言,需要花更多的时间登录,访问网络资源的速度也很慢。如果在分支机构网络中部署单独的域控制器,则就无法很好地实现统一管理。为了便于远程用户进行身份验证,需要在分支结构中部署一台只读域控制器,远程用户访问内部网络共享资源时可以在本地完成身份验证,提高网络安全性。另外,为了减轻网络管理员负担,需要将管理权限分配给不同的用户账户。

文件服务是面向所有客户端的,不同的共享资源安全需求不同,因此需要对不同的用户账户或组分配相应的访问权限。对于网络中重要的机密文件,需要严格限制用户的访问权限。由于企业内部的某些 Web 应用安全性要求较高,因此需要对 HTTP 传输进行 SSL 加

密传输。

3.1.3 解决方案

应用系统的安全跟具体应用有关，涉及很多方面，应该是动态的、不断变化的。本章主要解决网络中运行的网络服务的安全性。

1. 活动目录安全

可以通过如下措施加强域控制器的安全性。

(1) 部署只读域控制器。在企业的分支机构中部署只读域控制器，一方面可以确保域控制器数据库的物理安全；另一方面也可以加快远程用户的登录和访问速度。

(2) 重定向目录数据库。将活动目录数据库重定向到系统分区之外的其他磁盘分区或物理磁盘，可以避免系统故障对目录数据库的危害。

(3) 权限委派。将重要的网络管理员操作权限分配给不同的用户账户，既可以减轻管理员工作负担，又可以提升网络安全性。

(4) 域用户账户安全。为所有域用户账户设置安全密码，并严格限制登录时间和登录计算机，避免用户随意登录带来的危害。

(5) 灵活运用组。Windows 域中的组，则可以帮助管理员统一设置某些对象的权限，简化操作的复杂性，降低管理难度。

2. 文件服务安全

可以通过如下措施实现文件服务的安全。

(1) 配置 NTFS 访问权限。除了为文件服务器上的共享资源配置共享访问权限之外，还必须为不同的用户和组配置 NTFS 访问权限。

(2) 配置磁盘配额。通过为用户账户启用磁盘配额，可以严格限制用户账户在文件服务器上的写入操作，避免文件服务器存储空间的滥用。

(3) 文件屏蔽。限制用户可以向文件服务器上写入的文件类型。

3. IIS 服务安全

IIS 7.0 提供了丰富的身份验证机制，对于安全性要求较高的 Web 应用可以通过配置安全 Web 站点，实现 SSL 加密传输，充分确保客户端身份的真实性以及网络传输的安全性。

3.2 活动目录安全

活动目录服务是企业网络的重要服务，可以帮助管理员统一管理网络资源，例如可以根据网络用户的身份进行逻辑划分，分别赋予相应的访问权限，其目的在于提供有效、灵活的信息管理。Windows Server 2008 系统中的活动目录服务变化比较大，管理员可以通过 Active Directory 域服务控制台，统一管理域中的所有域控制器，包括登录处理、身份验证、目录搜索、重新启动等。只读域控制器可以充分确保目录数据库的安全性和可靠性。

3.2.1 只读域控制器

只读域控制器(RODC)是在 Windows Server 2008 系统提供的新型域控制器，可以帮助用户在物理安全得不到保证的情况下，部署域控制器并确保其安全性，例如该企业网络中的

分公司网络。RODC 包含了活动目录数据库的只读部分，可以帮助用户确保网络环境安全。域控制器是分支机构中最薄弱的环节。使用 RODC，可以将可写域控制器移到合适的数据中心，使用 RODC 替代分支机构中的可写域控制器，从而降低安全风险。

1. 查看缓存账户

默认情况下，安装 RODC 过程中，已经为部分用户账户创建了密码复制策略，可以使用如下方法查看 RODC 默认的账户缓存机制。

在 RODC 上，依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开“Active Directory 用户和计算机”窗口。此时连接到的域控制器状态为“只读”。依次选择 coolpen. net→Domain Controllers 选项，双击 RODC 显示“RODC 属性”对话框，切换到如图 3-1 所示的“密码复制策略”选项卡。

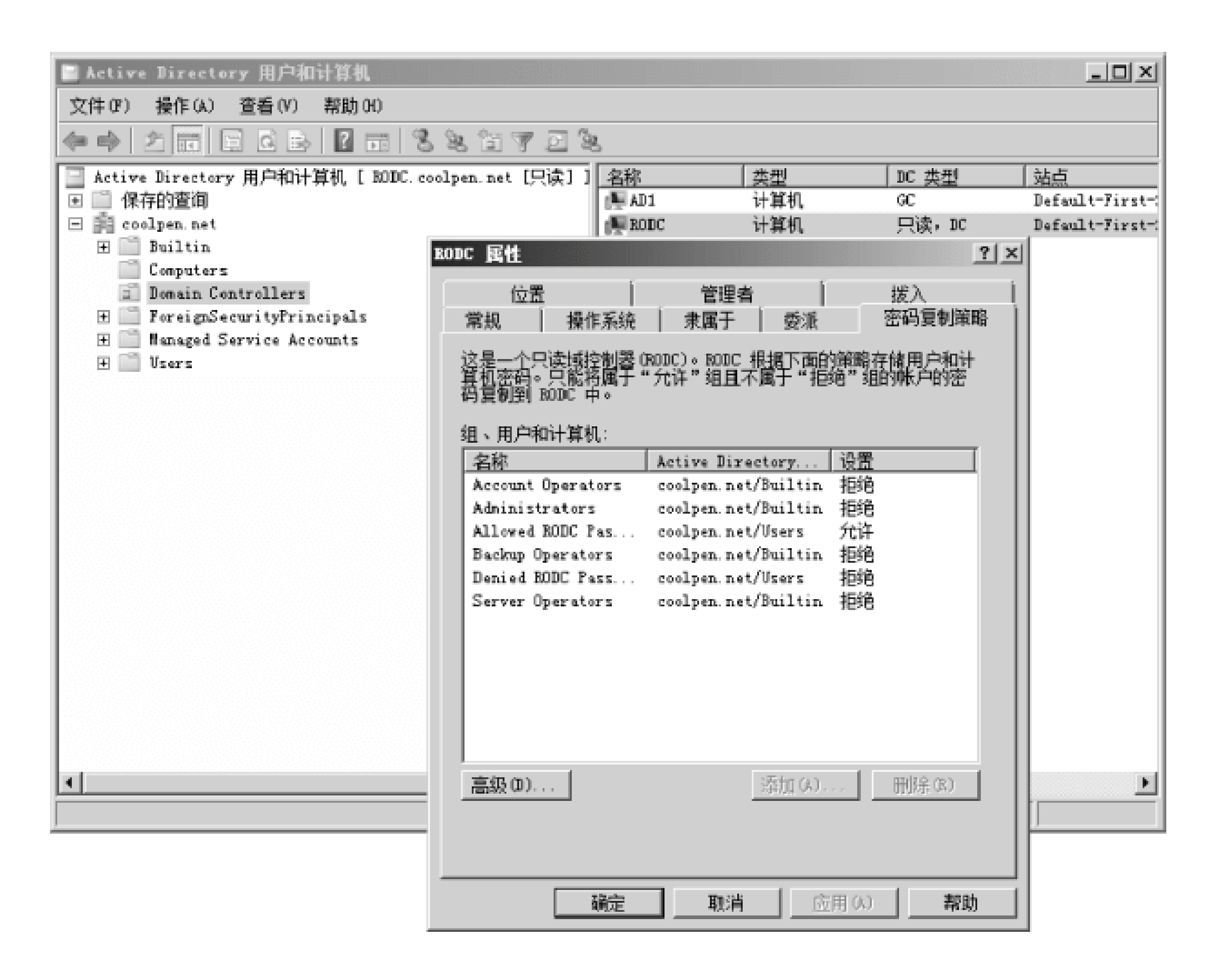


图 3-1　“密码复制策略”选项卡

提示：单击“高级”按钮，显示如图 3-2 所示的“以下项目的高级密码复制策略 RODC”对话框，这里显示的是密码复制策略的高级功能，用户可以根据需要选用。在“策略使用率”选项卡的“显示满足下列条件的用户和计算机”下拉列表框中，包括如下选项。

（1）选择“其密码已存储在此只读域控制器中的账户”选项，除了 RODC 自身的计算机账户和 Kerberos 票据授权（KRBTGT）账户之外，默认情况下没有缓存任何账户的密码。

（2）选择“已通过此只读域控制器身份验证的账户”选项，显示在 RODC 进行身份验证的用户以及计算机，通过此列表确定允许哪些账户的密码，在此 RODC 域控制器中进行缓存。

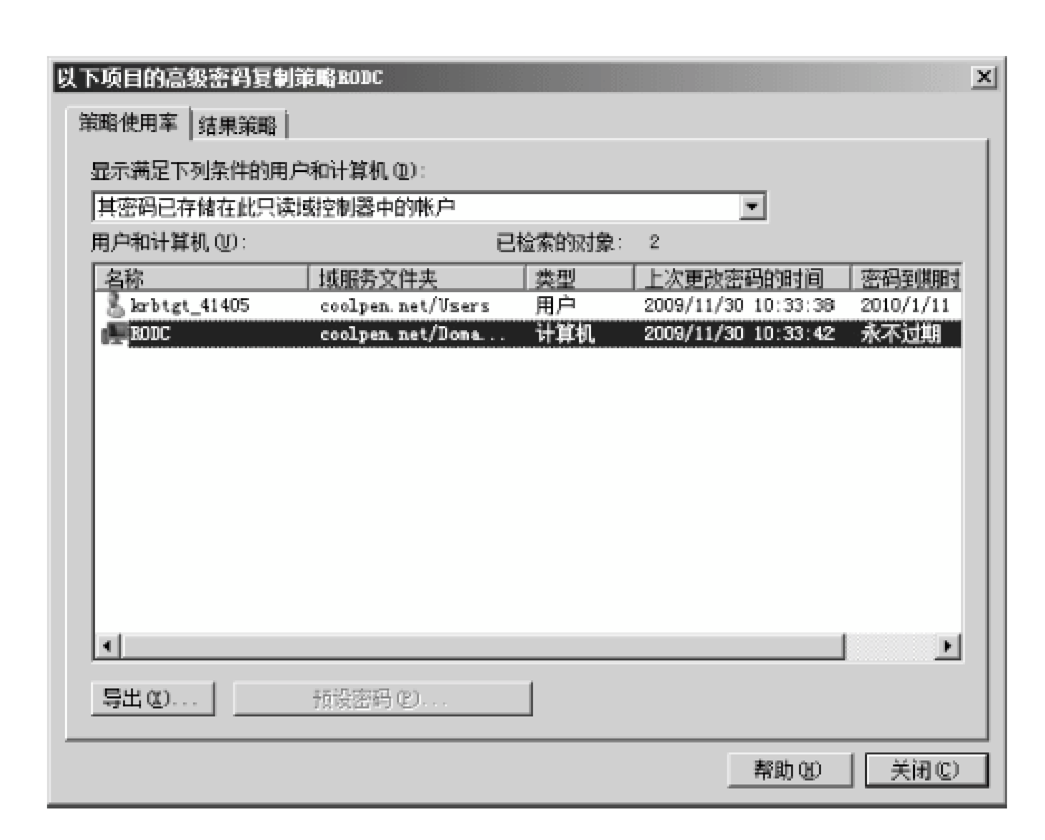


图 3-2　“以下项目的高级密码复制策略 RODC”对话框

2. 添加缓存账户

在源域控制器上，可以设置允许在 RODC

上缓存的用户分支机构。建议为分支机构创建单独的组织单位，在该组织单位下创建组，组的创建规则建议符合企业的行政管理架构，以降低管理的复杂度。例如，将本项目中分支机构的所有用户和组规划在“分支机构”组织单位中，现在需要将所有销售员用户账户缓存到RODC中，销售员账户隶属于xiaoshou组。

（1）在源域控制器上，打开“Active Directory用户和计算机”窗口，依次展开coolpen.net→Domain Controllers选项，双击RODC，打开“RODC属性”对话框，切换至如图3-3所示的“密码复制策略”选项卡。

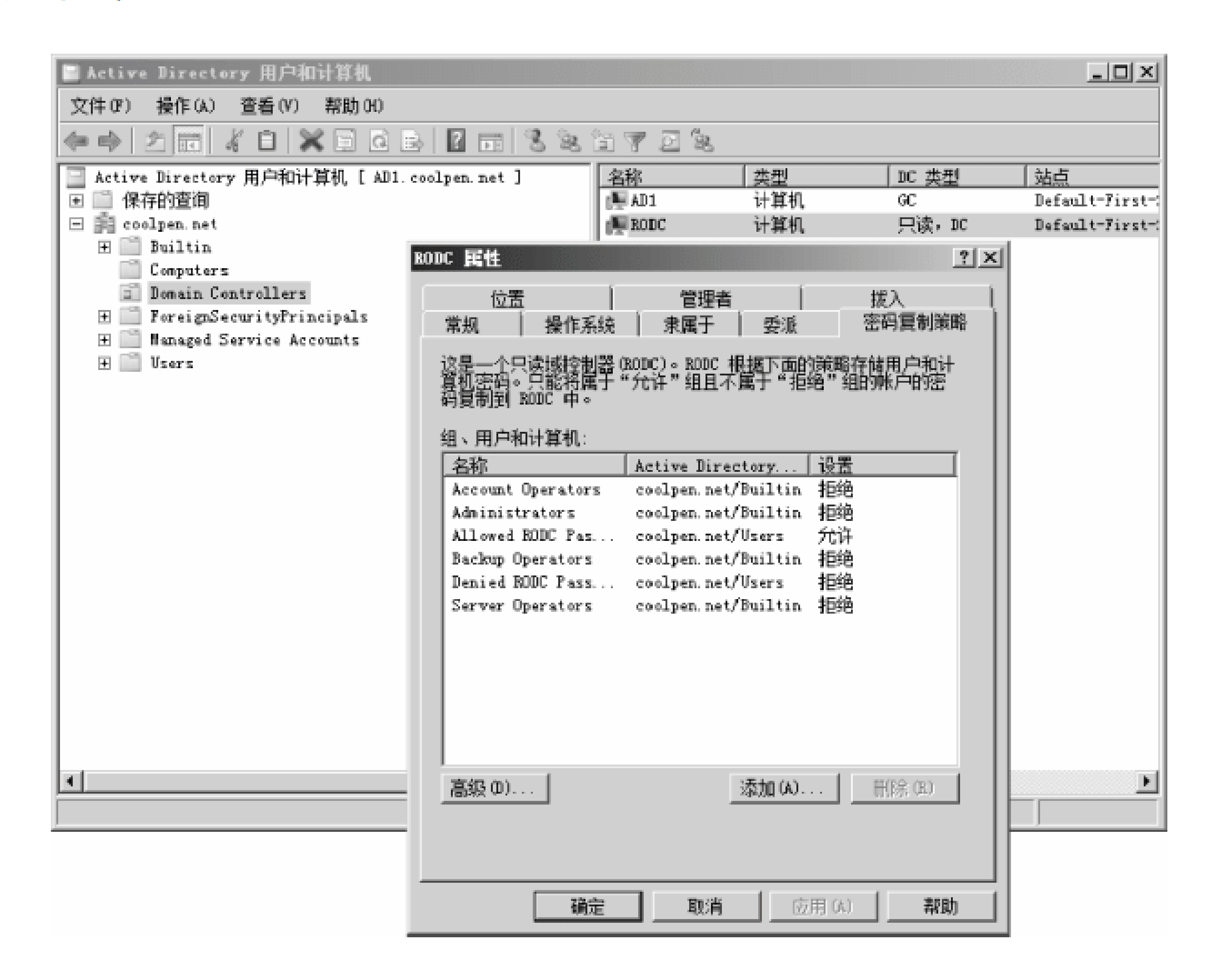


图3-3 “密码复制策略”选项卡

（2）单击“添加”按钮，显示如图3-4所示的“添加组、用户和计算机”对话框。设置RODC域控制器中允许或者拒绝缓存的组、用户和计算机，这里选中“允许该账户的密码复制到此RODC中”单选按钮。

（3）单击“确定”按钮，显示“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入想要添加的域用户账户。单击“确定”按钮，关闭“选择用户、计算机或组”对话框，返回到“RODC属性”对话框，所选用户账户已被添加到列表中，如图3-5所示。

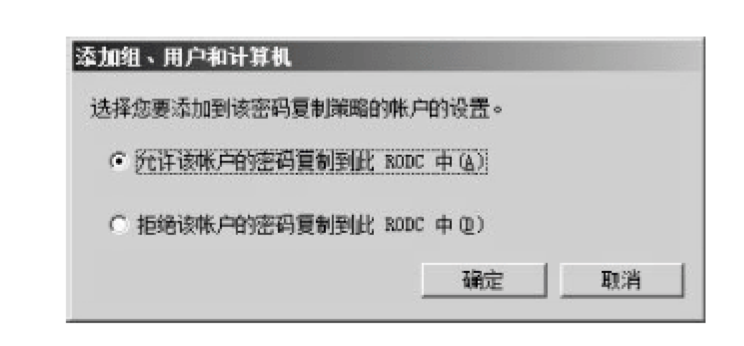


图3-4 “添加组、用户和计算机”对话框

（4）单击“应用”按钮，设置生效。

3. 预设密码

预设密码是将用户或计算机账户的密码缓存到RODC中，如果希望在没有域控制器可用的情况下，用户依然可以通过RODC登录，则用户账户的密码和用户登录的计算机账户的密码都必须存储在RODC上。缓存成功的用户账户或计算机账户，在域控制器脱机的情况下，可以通过RODC直接登录进行身份验证。例如，接下来将分支机构中的管理员用户账户和密码都缓存在RODC上。

（1）在源域控制器上，打开“Active Directory用户和计算机”窗口，打开“RODC属性”对话框，“密码复制策略”选项卡，单击“高级”按钮，显示如图3-6所示的“以下项目的高级密

码复制策略 RODC”对话框，默认显示“策略使用率”选项卡，此时的“预设密码”功能是可以编辑的。



图 3-5　允许将指定组的账户密码复制到 RODC 中



图 3-6　“以下项目的高级密码复制策略 RODC”对话框

(2) 单击“预设密码”按钮，显示如图 3-7 所示的“选择用户或计算机”对话框。在“输入对象名称来选择(示例)”文本框中，输入需要预设密码的用户或者计算机账户。

注意：操作之前，必须确保被预设密码的用户账户的密码已允许复制到 RODC 中，即添加到“密码复制策略”的“组、用户和计算机”列表中，否则无法为其预设密码。

(3) 单击“确定”按钮，显示如图 3-8 所示的“预填充密码”对话框。单击“是”按钮，即可成功完成指定用户账户的预设密码设置。



图 3-7　“选择用户或计算机”对话框

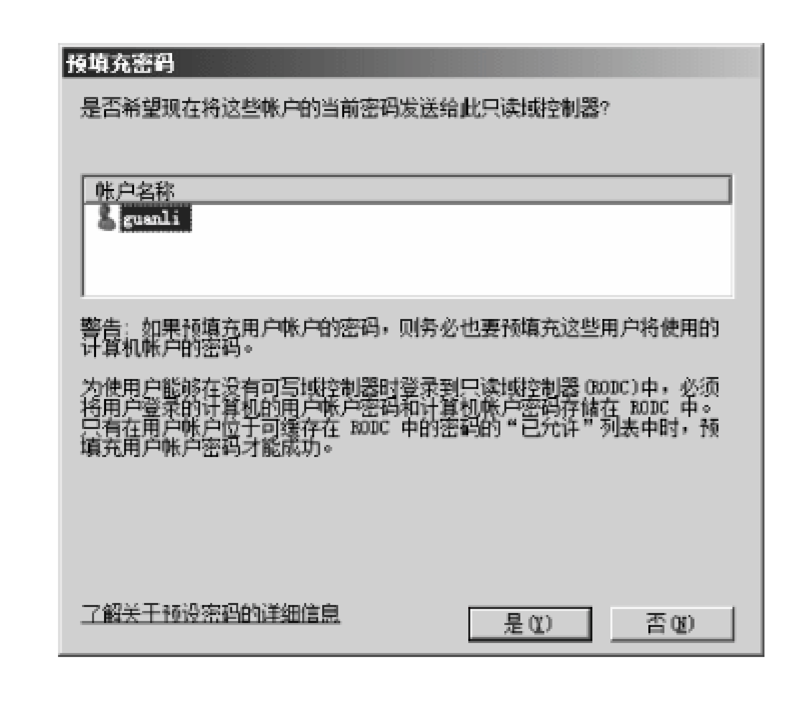


图 3-8　“预填充密码”对话框

3.2.2　重启 ADDS

在 Microsoft Windows 2000 Server 操作系统和 Windows Server 2003 操作系统的 Active Directory 中，对数据库进行脱机碎片整理时，需要在目录服务还原模式下重新启动域控制器。此外，应用安全更新通常也需要重新启动域控制器。但是在 Windows Server 2008 中，管理员可以停止并重新启动 ADDS，这样便能够更快速地执行脱机 ADDS 操作。

(1) 在“服务”管理窗口,双击 Active Directory Domain Services,显示如图 3-9 所示的“Active Directory Domain Services 的属性(本地计算机)”对话框。

(2) 单击“停止”按钮,显示如图 3-10 所示的“停止其他服务”对话框,在列表中显示了与该服务相关联的其他服务。



图 3-9 “Active Directory Domain Services 的属性(本地计算机)”对话框



图 3-10 “停止其他服务”对话框

(3) 单击“是”按钮,确认停止服务即可。

若要重新启动该服务,在“Active Directory Domain Services 的属性(本地计算机)”对话框中,单击“启动”按钮即可。

3.2.3 SYSVOL 安全

SYSVOL 是域中每台域控制器上文件系统中的文件夹和重分析点的集合。SYSVOL 存储重要组策略对象(GPO)策略和脚本。文件复制服务(FRS)将这些策略和脚本同步到域中的其他域控制器中。SYSVOL 目录的安全性直接决定域控制器乃至网络的安全。

1. SYSVOL 重定向

Windows Server 2003 提供两种方法可以完成 SYSVOL 共享文件夹的重定向。

(1) 使用 Active Directory 向导移动 SYSVOL。首先,需要降级域控制器,然后再对其升级,同时使用新的目录保存 SYSVOL 目录即可。不推荐使用这种方法。

(2) 手动重定向 SYSVOL 文件夹。本节示例就是通过这种方法实现的。

手动重定向 SYSVOL 的步骤如下。

(1) 查看 SYSVOL 默认位置,在命令提示符下,输入如下命令:

```
net share
```

按 Enter 键,命令行成功执行,执行结果如图 3-11 所示。SYSVOL 的默认位置为:C:\WINDOWS\SYSVOL\sysvol。



图 3-11 net share 执行结果

(2) 查看当前域的复制伙伴是否正常。在命令提示符下,输入如下命令:

dcdiag /test:replications

按 Enter 键,命令行成功执行,执行结果如图 3-12 所示,当前的复制链接,通过检查。



图 3-12 查看当前域的复制伙伴是否正常

(3) 查看当前域的 NetLogon 服务是否正常。在命令提示符下,输入如下命令:

dcdiag /test:netlogons

按 Enter 键,命令行成功执行,执行结果如图 3-13 所示,当前的 NetLogon 服务正常。

(4) 停止 FRS 文件复制服务。在命令提示符下,输入如下命令:

net stop ntfrs

按 Enter 键,命令行成功执行,执行结果如图 3-14 所示。



图 3-13 查看当前域的 NetLogon 服务是否正常



图 3-14 停止 FRS 服务

(5) 在目标位置建立新的 SYSVOL 存储新位置,如 D:\new sysvol,并将 SYSVOL 文件夹中的内容复制到新的文件夹中,如图 3-15 所示。

(6) 修改注册表,更改系统默认的 SYSVOL 的存储位置。打开注册表编辑器,展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\

Parameters 键值，右击 SYSVOL 选项，在弹出的快捷菜单中选择“修改”选项，显示“编辑字符串”对话框。在“数值数据”文本框中，输入新的文件夹的位置 D:\new sysvol，如图 3-16 所示。最后，单击“确定”按钮，保存修改的数据。

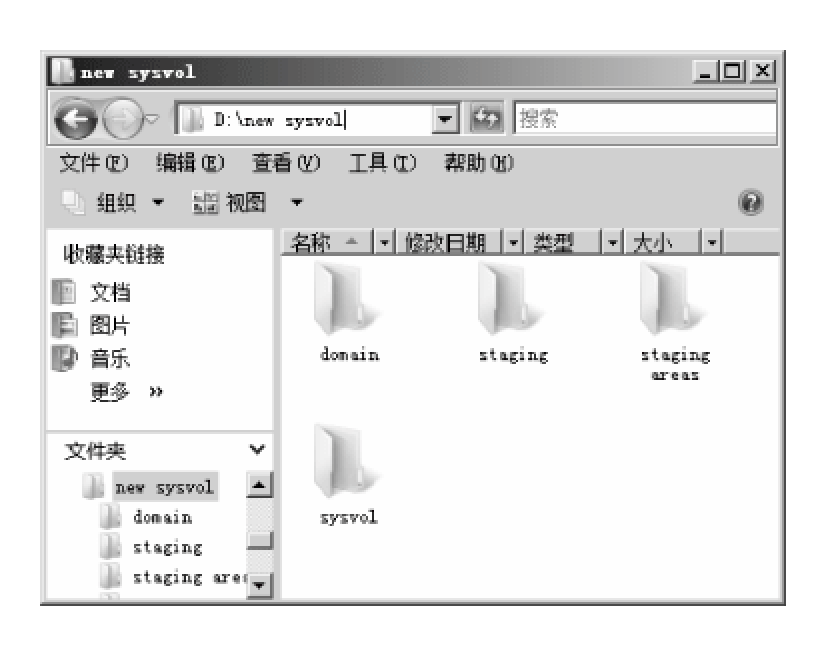


图 3-15 新的 SYSVOL 目标文件夹

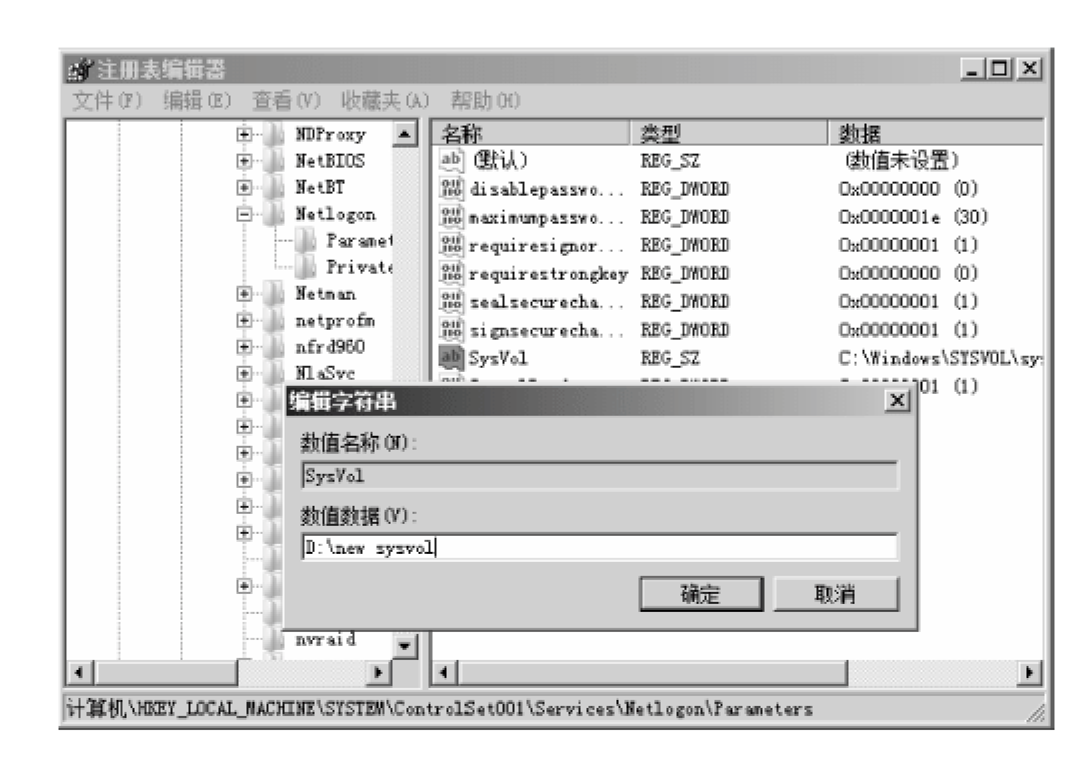


图 3-16 修改注册表设置

（7）使用 ADSI Edit 工具修改 Active Directory 数据库中的 SYSVOL 存储位置信息。单击“开始”按钮，选择“运行”命令，在“运行”对话框中，输入 adsi edit，单击“确定”按钮，打开 ADSI Edit 窗口，如图 3-17 所示。

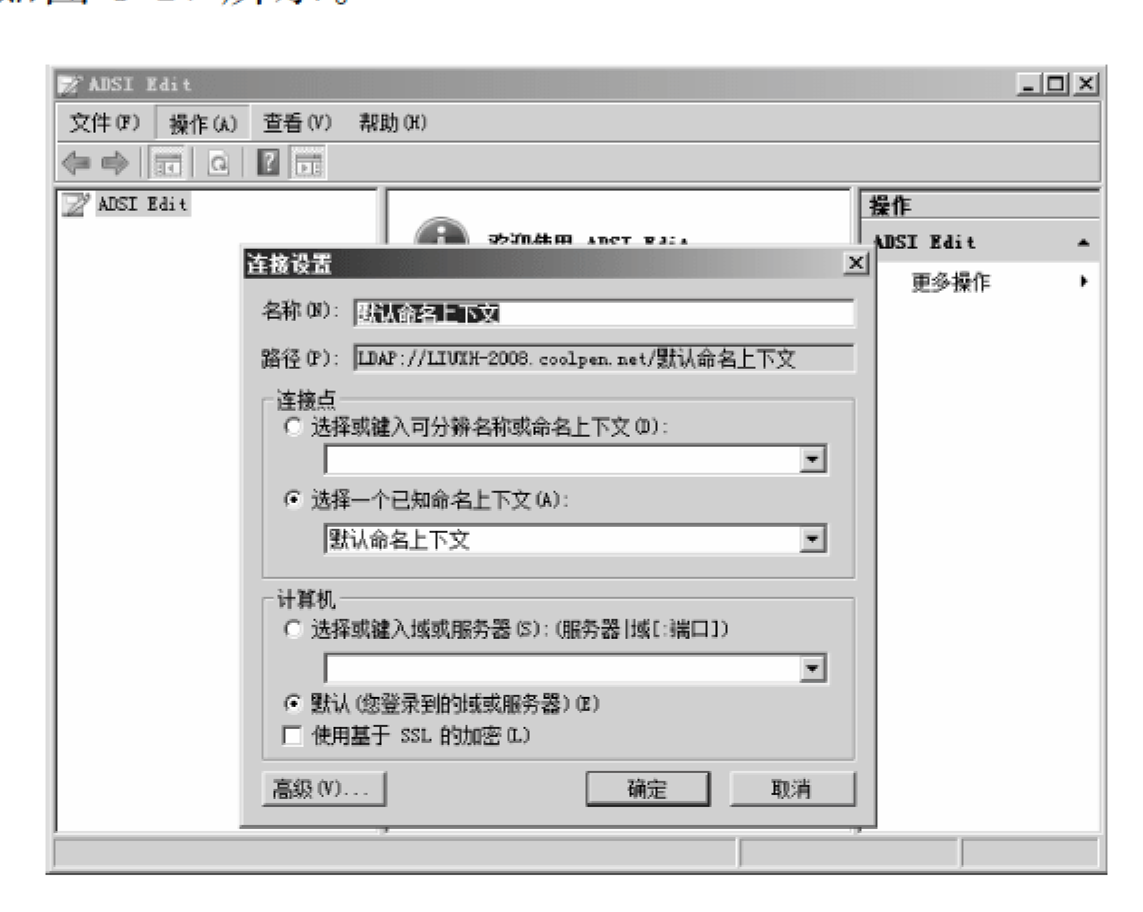


图 3-17 ADSI Edit 窗口

（8）依次展开 DC=coolpen，DC=net→OU=Domain Controllers→CN=AD1→CN=NTFRS Subscriptions 选项，右击 CN=Domain System Volume（SYSVOL share）选项，选择快捷菜单中的“属性”选项，显示如图 3-18 所示的“CN = Domain System Volume（SYSVOL share）属性”对话框。单击“筛选器”按钮，取消“可选”选项，即只查看“强制”和“仅系统”属性信息。

（9）在“属性”列表中，选中 fRSRootPath 属性，单击“编辑”按钮，显示如图 3-19 所示的“字符串属性编辑器”对话框，在“值”文本框中，输入新建的目标文件夹的位置 d:\new sysvol 即可。单击“确定”按钮保存设置即可。按照相同的方法，将 fRSStagingPath 属性的值修改为 d:\new sysvol 即可，此处不再赘述。

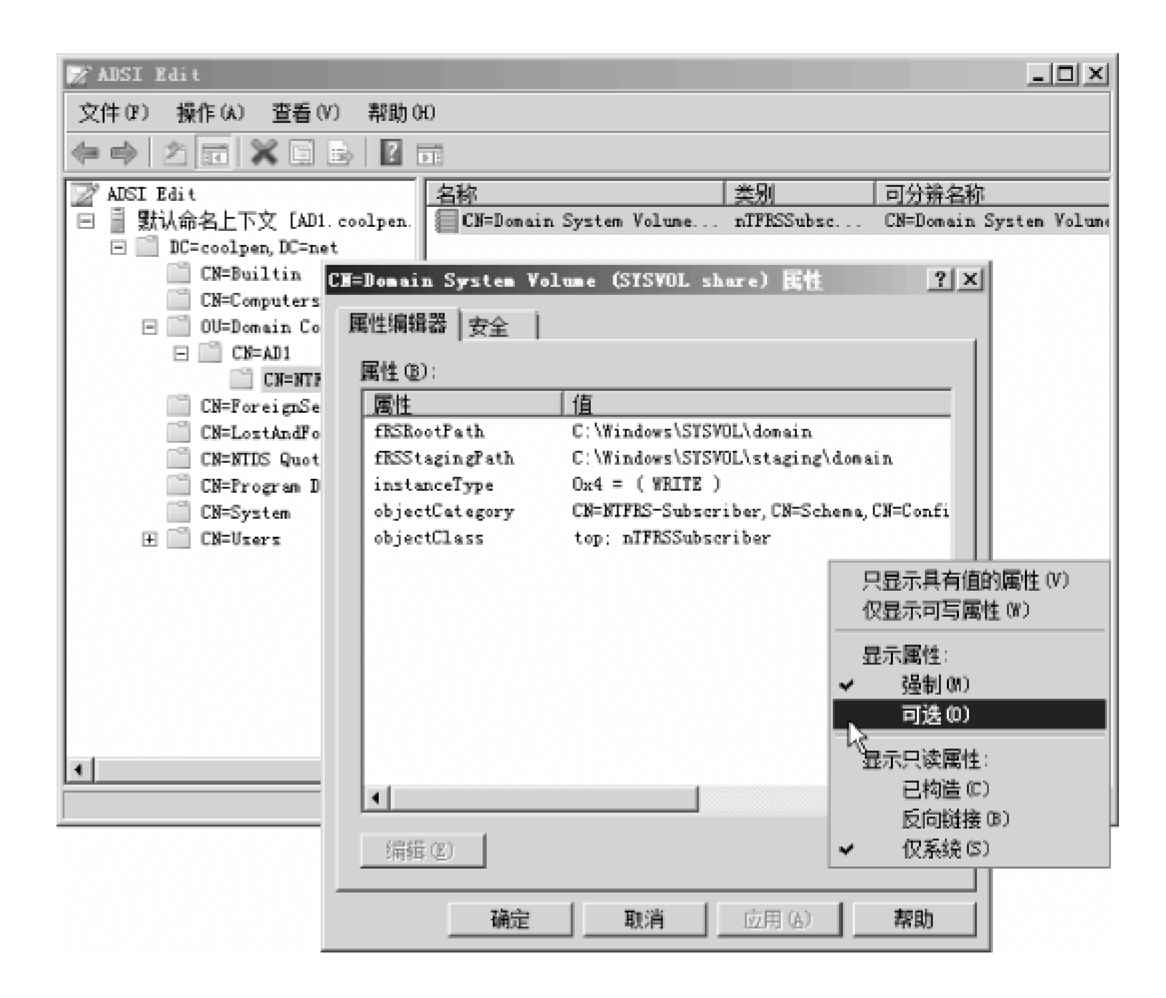


图 3-18 “CN＝Domain System Volume(SYSVOL share)属性”对话框

(10) 创建 FRS 文件复制服务的挂接点。在命令提示符下，进入 FRS 服务的默认位置 C:\WINDOWS\SYSVOL，输入如下命令：

```
mklink /J coolpen.net d:\"new sysvol"
```

按 Enter 键，命令行成功执行，执行结果如图 3-20 所示。



图 3-19 “字符串属性编辑器”对话框



图 3-20 创建 FRS 文件复制服务的挂接点

(11) 设置 FRS 服务为不可信。域控制器离线后，NTFRS 服务停止工作，需要将域控制器上 FRS 服务设置为不可信。在联机时需要马上从其他的域控制器复制 SYSVOL 文件夹中的内容，同步完成后域控制器上 SYSVOL 即可正常工作。打开注册表编辑器。展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup 键值，右击右窗格中的 BurFlags 选项，选择快捷菜单中的“修改”选项，显示如图 3-21 所示的“编辑 DWORD(32 位)值”对话框，在“数值数据”文本框中输入 D2，单击“确定”按钮保存。

(12) 重新启动 NTFRS 服务。在命令提示符下，输入如下命令：

```
net start ntfrs
```

按 Enter 键，命令行成功执行，执行结果如图 3-22 所示。

(13) 检查共享。在命令提示符下，输入如下命令：

```
net share
```

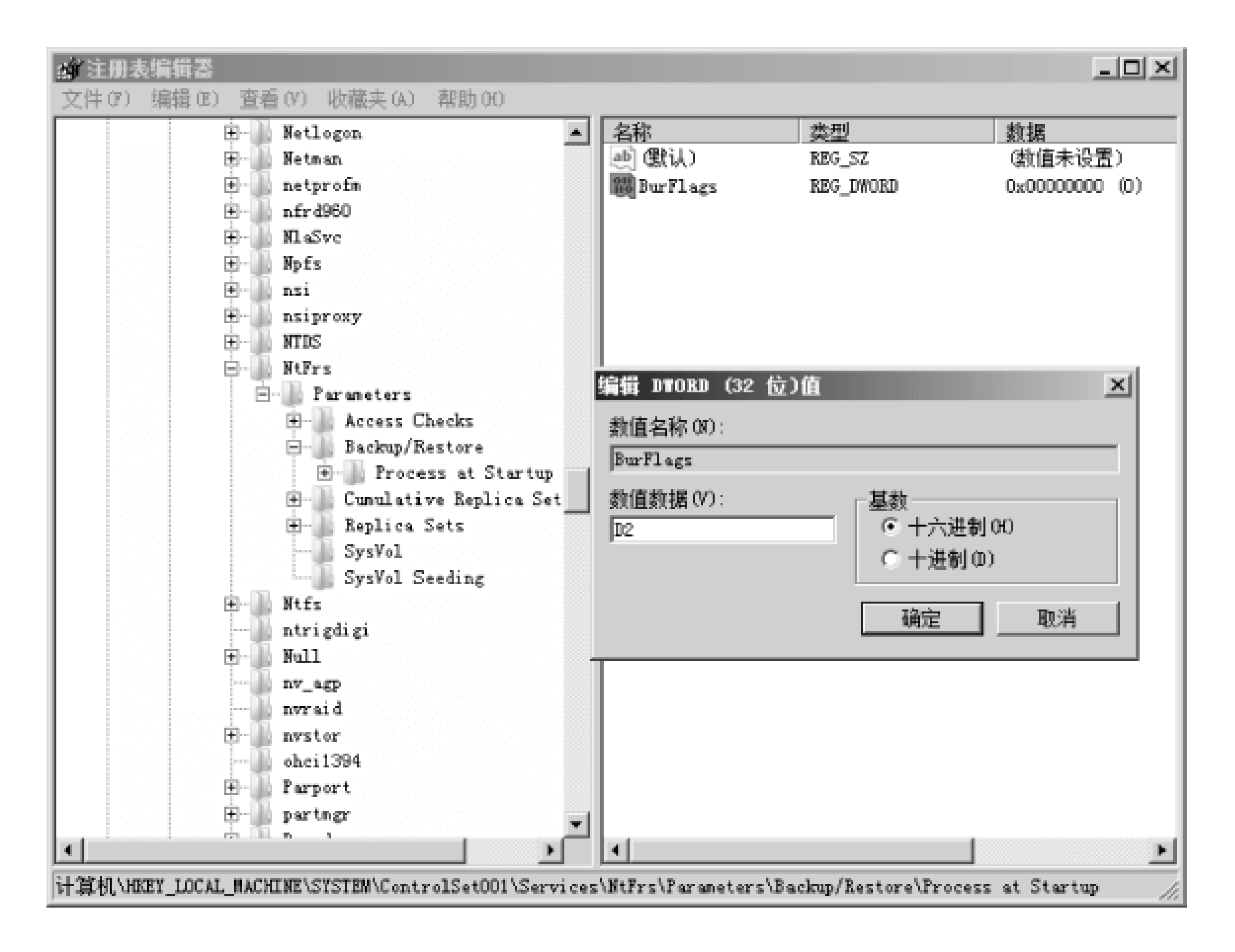


图 3-21 “编辑 DWORD(32 位)值”对话框

按 Enter 键,命令行成功执行,执行结果如图 3-23 所示。SYSVOL 共享的位置已经由 C:\WINDOWS\SYSVOL\sysvol 重定向到了 D:\new sysvol 目录。



图 3-22 启动服务



图 3-23 执行结果

2. 更改 SYSVOL 存储空间

SYSVOL 文件夹中的 Staging Area 目录存储的是 NTFRS 文件服务复制服务的文件交换区域,需要复制的信息首先放在 Staging Area 区域,作为中转存储区域。SYSVOL 存储空间的默认大小为 10MB,最大 675MB。如果 Active Directory 中部署了文件分布式系统(DFS),则 DFS 使用 Staging Area 目录作为交换空间,当 DFS 存储的单个文件大小超过 675MB 时,则 Staging Area 无法正常使用,导致服务失败。为此,需要更改 SYSVOL 存储空间的上限值。

打开“注册表编辑器”窗口,依次展开 HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ NtFrs\Parameters 键值,右击 Staging Space Limit in KB 选项,选择快捷菜单中的“修改”选项,显示如图 3-24 所示的“编辑 DWORD(32 位)值”对话框。在“数值数据”文本框中,输入需要设置的交换区域的大小即可,例如 20000000,交换区域的空间值按照 KB 计算。

单击“确定”按钮,即可完成 SYSVOL 交换区域大小的设置。重新启动域控制器,更改

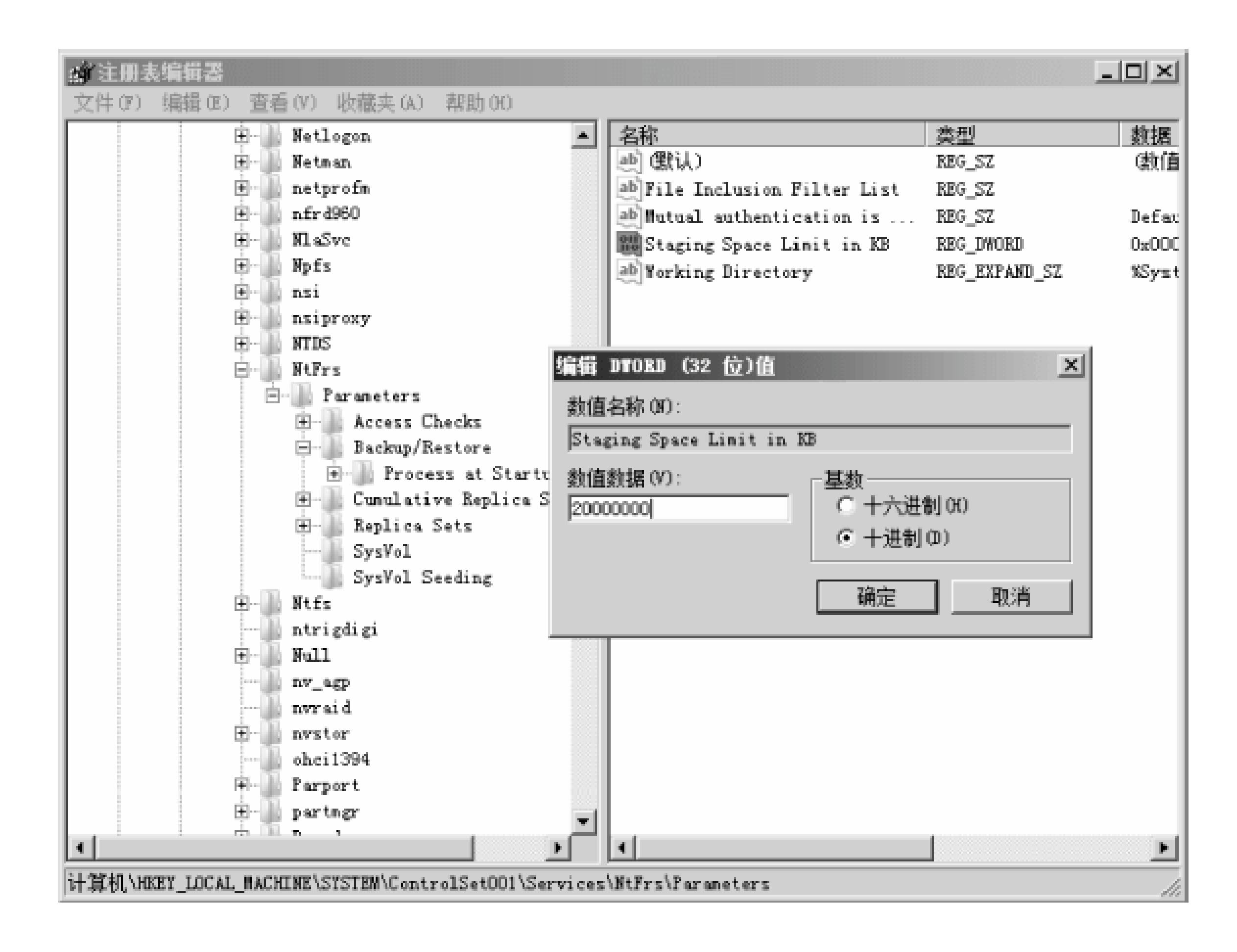


图 3-24 “编辑 DWORD(32 位)值”对话框

的交换区域生效。

3.2.4 管理员授权

为了确保企业网络的安全，管理员可以将管理权限指派到不同的用户账户，避免权限过于集中。对于普通而言，权限最小化的分配方案也是非常有效的，平时仅赋予用户普通登录和访问权限即可，如有特殊需求时可以通知管理员临时获得授权，既可以避免权限滥用，又可以确保网络访问的安全。

1. 权限委派

在 Windows Server 2008 系统的 Active Directory 用户和计算机中，可以通过高级功能模式和控制委派向导两种方式委派权限。例如，将向“员工”组织单位添加用户账户的权限，委派给“网络管理部”中的某个用户。

(1) 打开“Active Directory 用户和计算机”窗口，右击“阅览室”并选择快捷菜单中的“委派控制”选项，启动“控制委派向导”，单击“下一步”按钮，显示“用户或组”对话框。在这里需要将用于承担委派权限的用户账户添加到“选定的用户和组”列表中。单击“添加”按钮，显示如图 3-25 所示的“选择用户、计算机或组”对话框，在“输入对象名称来选择(示例)”文本框中输入用户的名称 tianjl，然后单击“确定”按钮，即可添加该用户。

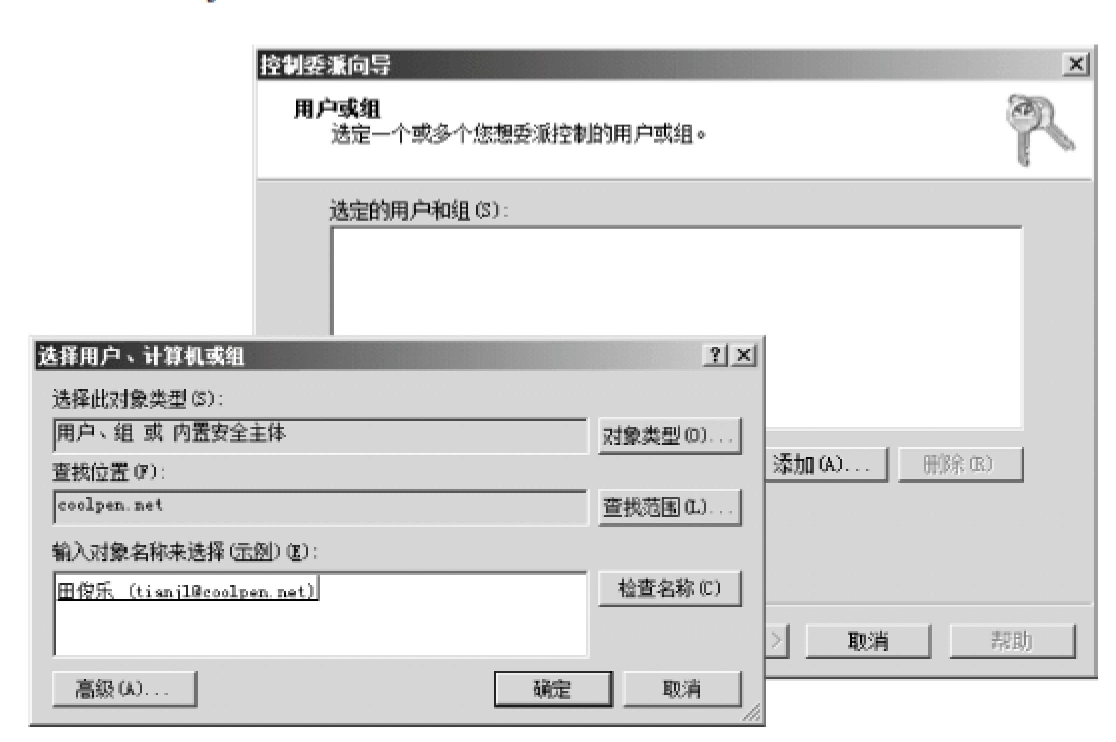


图 3-25 “选择用户、计算机或组”对话框

(2) 单击“下一步”按钮，显示如图 3-26 所示的“要委派的任务”对话框。在“委派下列常见任务”列表中，选中“创建、删除和管理用户账户”和“创建、删除和管理组”复选框。

提示：如果选中“创建自定义任务去委派”单选按钮，单击“下一步”按钮，则将显示如图 3-27 所示的“Active Directory 对象类型选择”对话框，这里对目录对象类型的划分更加详细，管理员可以更加准确地定位。

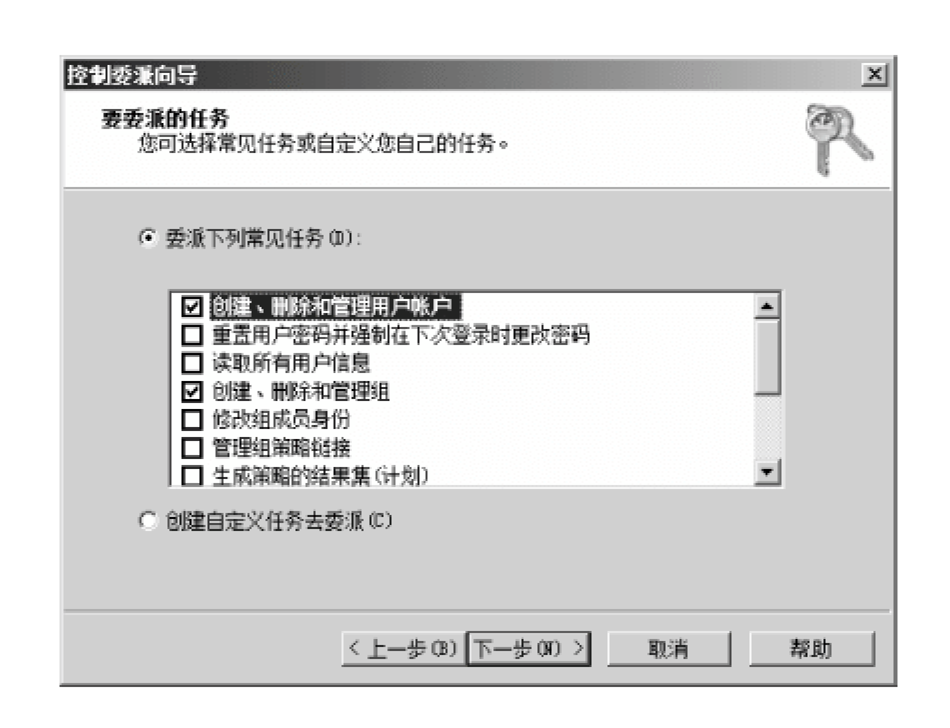


图 3-26 “要委派的任务”对话框

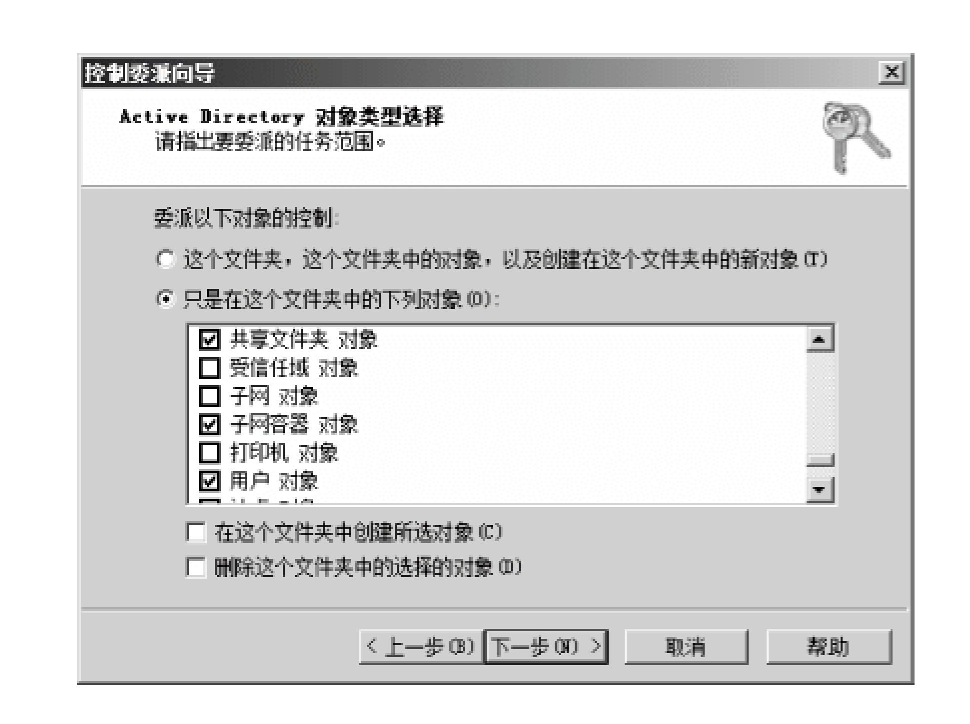


图 3-27 “Active Directory 对象类型选择”对话框

(3) 单击“下一步”按钮，显示“完成控制委派向导”对话框，并显示了前面所设置的信息。单击“完成”按钮，即可完成委派任务操作。

为了验证委派权限是否生效，可以在网络中任意工作站上，以田俊乐用户(对应用户账户为 tianjl)登录到域，并通过控制台，远程连接到域控制器，打开“Active Directory 用户和计算机”窗口。在“员工”组织单位上右击，会发现快捷菜单中的“新建”选项，如图 3-28 所示。默认情况下，普通用户账户在其他任何组织单位或容器上，都不会拥有该权限，即快捷菜单中不会出现“新建”选项。

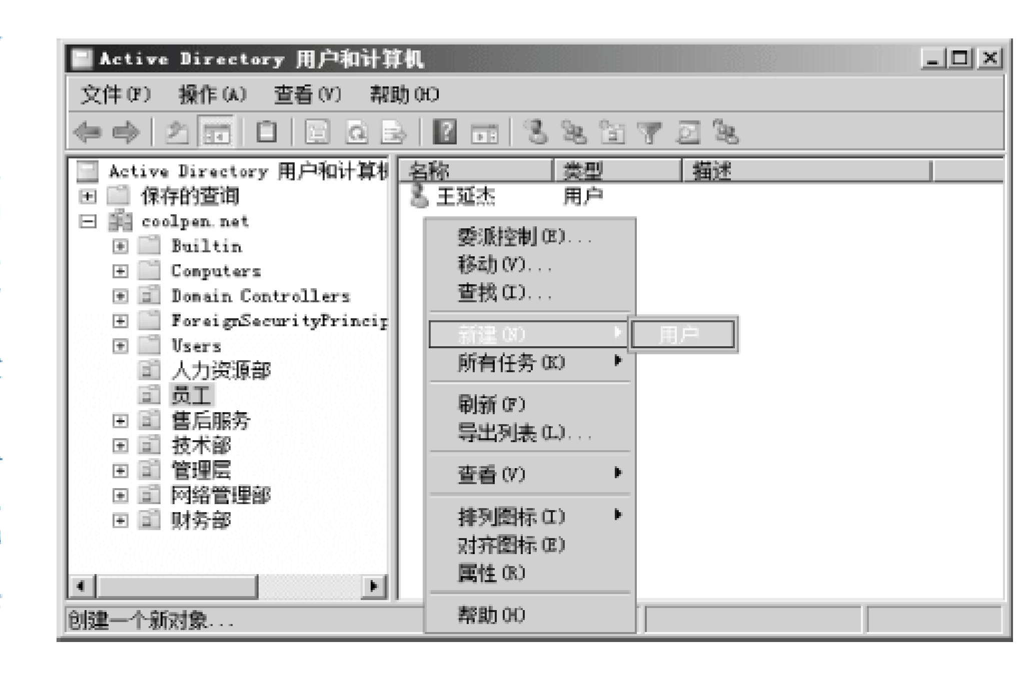


图 3-28 用户行使被委派的权限

注意：用于远程连接域控制器管理控制台的计算机，必须已安装 Active Directory 服务，否则无法添加“Active Directory 用户和计算机”管理单元。

委派的权限只能作用于目标对象，即不会自动传播到其所包含的子对象上。在本例中，tianjl 账户只能在“阅览室”组织单位中创建子对象，如 OU、用户、组等，但无法在这些子 OU 或组中继续创建对象。

2. 指派组管理权限

组是域网络管理中必不可少的，通过将组的管理权限指派给某个用户账户，可以大大减轻管理员的工作负担。需要注意的是，默认情况下，指定组管理员后，其他任何用户甚至管理员都将无法管理该组。

(1) 打开“Active Directory 用户和计算机”控制台，右击“临时员工”组并选择快捷菜单中的“属性”选项，显示“临时员工 属性”对话框，切换到“管理者”选项卡。单击“更改”按钮，显示如图 3-29 所示的“选择用户、联系人或组”对话框。在“输入要选择的对象名称(例如)”

文本框中，输入要指派的管理者的用户名或组名。需要注意的是，这里只能选择一个管理者，该管理者可以不属于当前组。

（2）单击“确定”按钮返回“管理者”选项卡，在“姓名”文本框中，显示了所添加的管理者用户名称，如图 3-30 所示。如果要清除管理者用户账户，单击“清除”按钮即可。




图 3-29　“选择用户、联系人或组”对话框

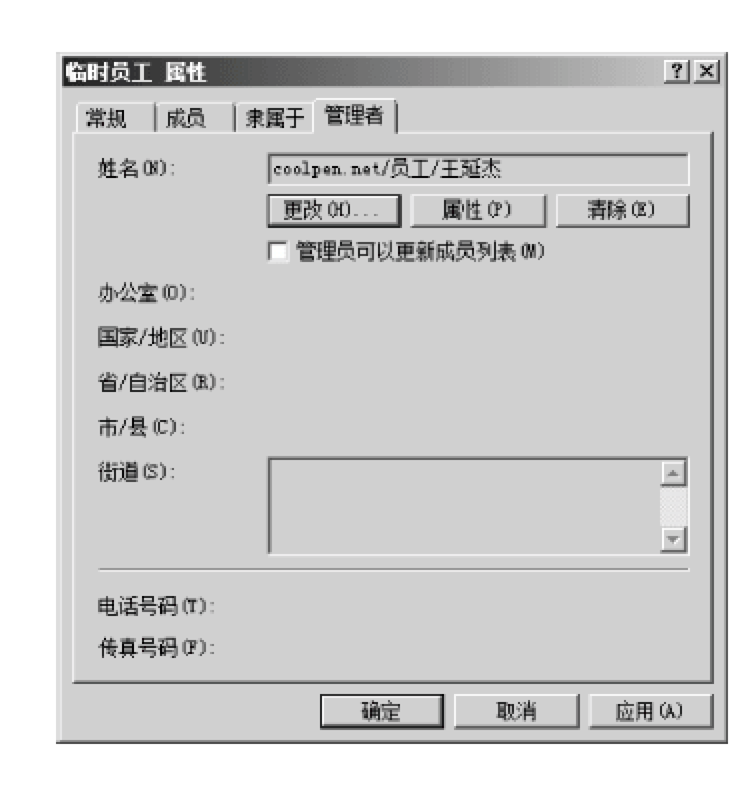


图 3-30　已指定管理者

提示：默认情况下，“管理员可以更新成员列表”复选框没有被选中，表示只有被指定的管理者才能管理该组，即使是域管理员也无此权限。如果选中该复选框，则允许管理员账户更新组成员列表。

（3）单击“确定”按钮，完成组的管理者的指派。

3.2.5　用户账户管理

域管理员是系统默认创建的，在应用过程中，管理员需要根据用户需要为其创建对应的用户账户，用户账户的权利代表了用户对网络资源的访问和操作权限。为防止用户账户被冒用，当用户离开或暂时不用时，管理员需要将其对应用户账户删除或停用。

1. 设置用户账户密码

普通用户账户忘记登录密码是时有发生的事，此时可以通知网络管理员或者被委派相关权限的用户账户，登录到域控制器重新修改登录密码即可。使用具有相关权限的管理员账户登录到域控制器，打开“Active Directory 用户和计算机”窗口。展开用户账户所在的组织单位，右击想要重置密码的用户账户，选择快捷菜单中的“重置密码”选项，显示如图 3-31 所示的“重置密码”对话框，在“新密码”和“确认密码”文本框中输入新密码，单击“确定”按钮即可。使用这种方法，也可以重设管理员账户的密码。

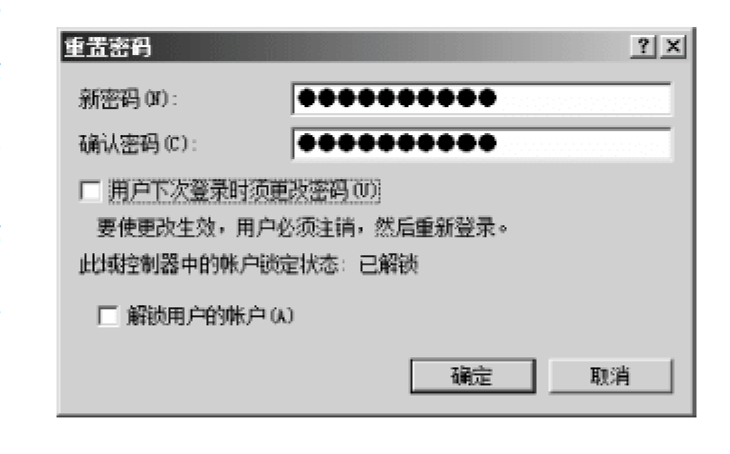


图 3-31　“重置密码”对话框

提示：如果当前账户已被锁定，则可以选中“解锁用户的账户”复选框，使密码更改立即生效。系统默认配置的安全策略，可能会限制用户更改密码的次数或登录次数，如果超出策略限制，则立即锁定账户，并等待一定时间后自动解锁。此时，对应用户可以告知管理员，由管理员登录到域控制器，使用“解锁用户的账户”方式为其重设密码并解锁账户。

2. 禁用或删除用户账户

以具有管理员权限的账户登录控制器,打开"Active Directory 用户和计算机"窗口,右击想要禁用的用户账户,选择快捷菜单中的"禁用账户"选项即可将其禁用,如图 3-32 所示。

用户账户被禁用以后,便不能再登录。如果想启用用户账户,则可以按照相同的方法,选择快捷菜单中的"启用账户"选项即可。如果账户不再使用,或需要重设所有权限,可将其删除,右击用户账户名,并选择快捷菜单中的"删除"选项即可删除该账户。

3. 限制用户可以登录的时间

默认情况下,域用户账户可以随时登录到域控制器,但是为了确保服务器系统以及网络的安全,应对用户账户的登录时间进行限制。该限制仅适用于域用户账户,本地用户账户登录系统时间无法限制。

(1) 在"Active Directory 用户和计算机"窗口中,双击要设置的用户,打开用户属性对话框,如图 3-33 所示。



图 3-32 禁用域用户账户

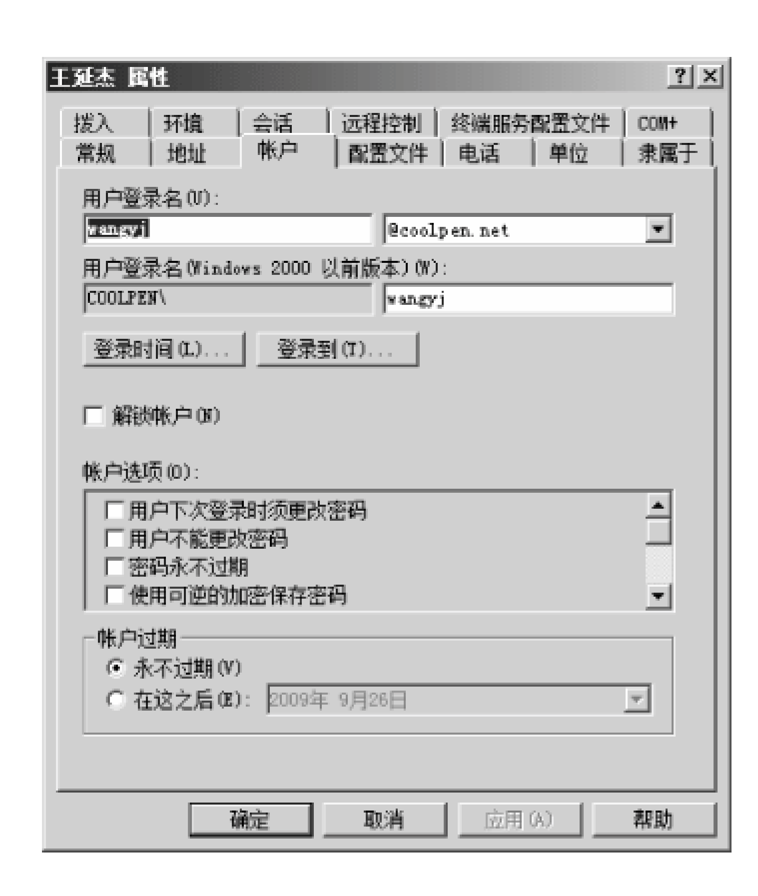


图 3-33 "王延杰 属性"对话框

(2) 单击"登录时间"按钮,显示如图 3-34 所示的"王延杰 的登录时间"对话框,默认允许在任何时间登录。

(3) 在登录时间分布表中,框选拒绝登录的时间范围,选中"拒绝登录"单选按钮,如图 3-35 所示。例如,本例中设置的是"王延杰"用户,在每周星期一到星期五的 7 点至 17 点范围内登录域。

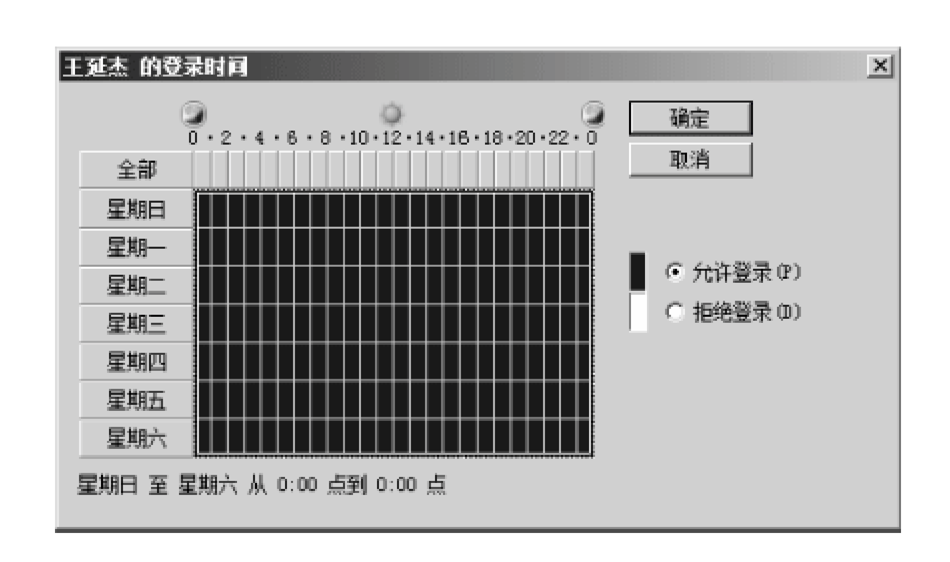


图 3-34 "王延杰 的登录时间"对话框

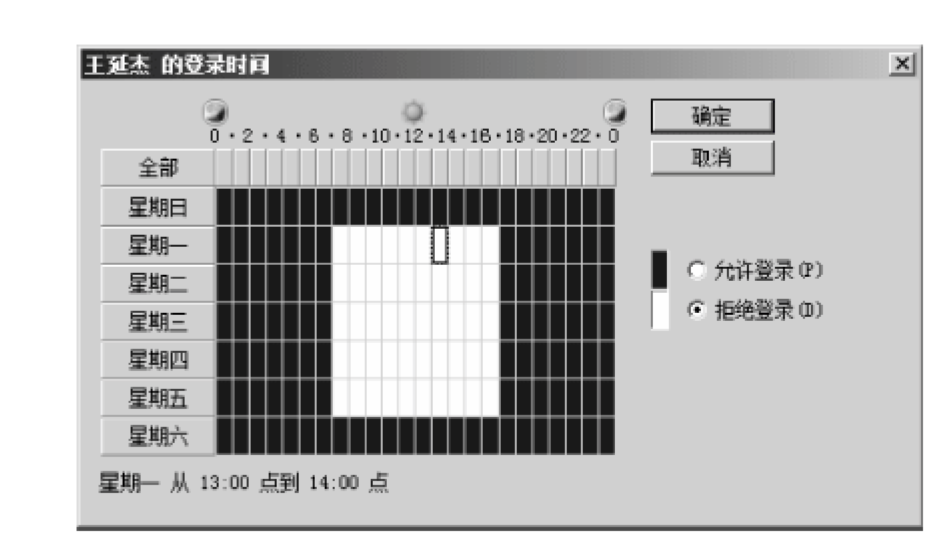


图 3-35 设置登录时间

（4）单击“确定”按钮，保存设置。

4. 限制用户可以登录的工作站

限制用户可以登录的工作站，是指限制用户账户只能从网络中指定的计算机上登录，访问 Active Directory 中的资源。默认情况下，域用户账户可以从网络中任意计算机上登录，通过将用户账户和登录计算机捆绑在一起，可以实施更加有效的安全管理措施。

（1）仍然以“王延杰”用户为例，在“王延杰 属性”对话框的“账户”选项卡中，单击“登录到”按钮，显示如图 3-36 所示的“登录工作站”对话框。默认选中“所有计算机”单选按钮，即允许用户登录网络中的所有计算机。

（2）选中“下列计算机”单选按钮，在“计算机名称”文本框中输入允许登录的工作站的 NetBIOS 名称，单击“添加”按钮添加到列表中，可以添加多个允许登录的工作站名称。

（3）单击“确定”按钮保存设置。

5. 恢复误删除的域用户

在 Windows Server 2008 的“Active Directory 用户和计算机”管理控制台中，没有提供对误删除的用户恢复功能。管理员可以借助 Adrestore. exe 工具，在命令行模式下恢复删除的用户，该工具支持 Windows Server 2000/2003/2008 系统中的活动目录，下载地址为 http://technet. microsoft. com/zh-cn/dd578429. aspx。例如，“王延杰”用户（对应账户为 wangyj）被误删除，则可以按照如下方法将其恢复。

（1）将 Adrestore. exe 复制到运行 ADDS 域服务的计算机中，选择“开始”→“所有程序”→“附件”→“命令提示符”选项，显示如图 3-37 所示的命令提示符窗口，并进入存储 Adrestore. exe 的文件夹。输入如下命令：

```
adrestore /r
```

按 Enter 键执行，显示如图 3-37 所示窗口，该命令列举活动目录中被删除的对象。



图 3-36　“登录工作站”对话框

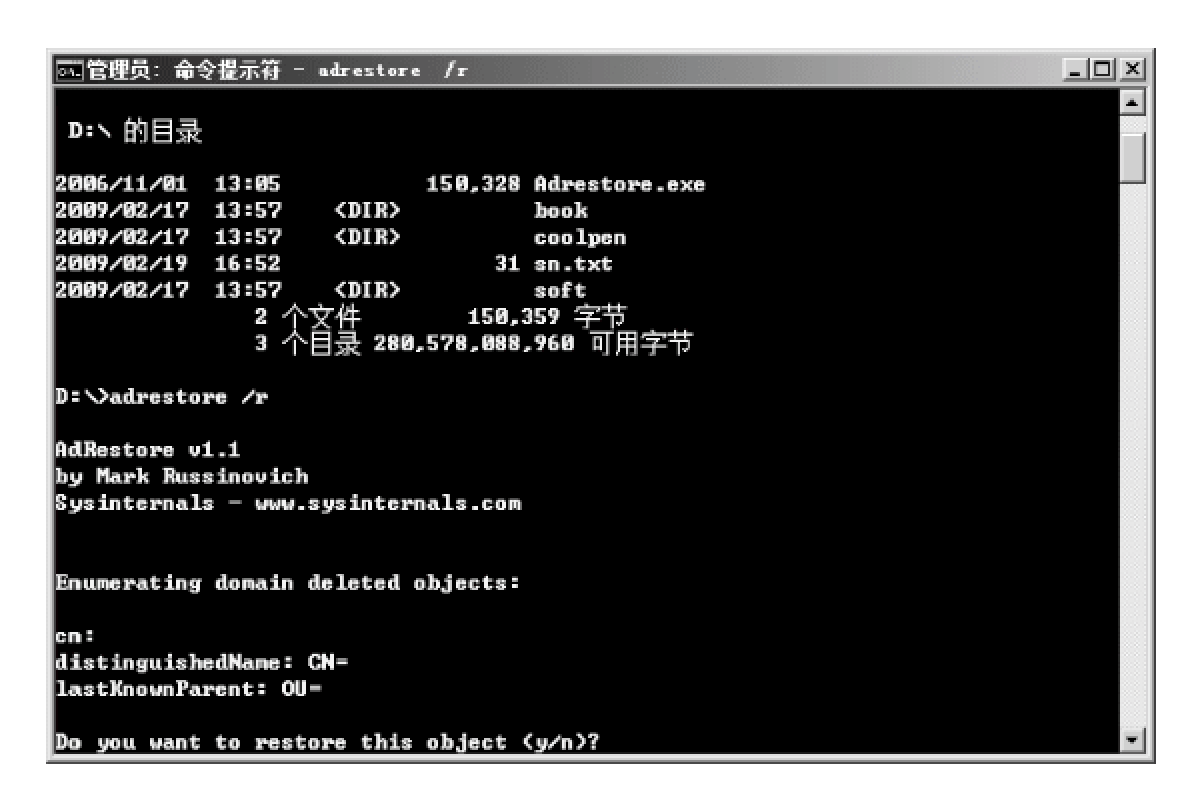


图 3-37　列举活动目录中被删除的对象

（2）输入 y 并按 Enter 键执行，恢复删除的用户信息，提示用户被成功恢复，如图 3-38 所示。同样的方法可以恢复其他被删除的 Active Directory 对象。

（3）打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→coolpen. net→“员工”选项，即可看到“王延杰”用户被成功恢复，默认情况下此用户账户的状态为“禁用”，如图 3-39 所示。



图 3-38 成功恢复误删除的用户账户



图 3-39 被删除用户已被恢复

(4) 恢复的账户需要重新设置密码,启用该账户即可完整恢复被删除的用户账户。

3.2.6 用户组管理

组作用域直接决定组中账户的应用范围,而组类型则决定用户账户可以行使的功能。应用过程中,管理员可以根据需要,更改域用户组的作用域和类型。需要注意的是,如果域功能级别为 Windows 2000 混合模式,则无法完成此过程。Windows Server 2008 系统的默认域功能级别为 Windows 2000 纯模式,并且已经删除了混合模式,所以可以直接更改。

打开"Active Directory 用户和计算机"控制台,双击欲更改的用户组(以"临时员工"组为例),显示如图 3-40 所示的"临时员工 属性"对话框,在"常规"选项卡的"组作用域"和"组类型"选项区域,重新选择指定的选项即可。



图 3-40 "临时员工 属性"对话框

在"Active Directory 用户和计算机"窗口中,右击要删除的组并选择快捷菜单中的"删除"选项,即可删除该组。需要注意的是,随着用户组的删除,通过该组所赋予成员账户的权限也会被删除,但组内的成员不会被删除。

3.2.7 知识链接:活动目录安全

1. 只读域控制器

(1) RODC 的优点

RODC 虽然是一个只读的域控制器,但本质上还是域控制器,具备域控制器的功能和优点,同时具有以下特点。

① 只读 Active Directory 数据库。RODC 上包含所有域对象和属性,与可读写域控制器不同的是,只能读取可读写域控制器中的数据,无法对 RODC 的 Active Directory 数据库进行更改。RODC 默认情况下,RODC 中不存储账户的密码。在不能保证域控制器安全性的情况下,可以通过 RODC 保证分支机构域安全性。

② 单向复制。可读写域控制器之间的复制是双向的,而 RODC 和可读写域控制器之间的复制是单向的,RODC 通过分布式文件系统(DFS)从可读写域控制器复制数据。

③ 密码缓存。默认情况下，RODC 上只存储本地的计算机账户和一个用于 RODC 特殊的 Kerberos 票据授权(KRBTGT)账户，此账户被可读写域控制器用来验证 RODC 身份。在可读写域控制器上启用密码缓存功能，即可在 RODC 上缓存所有域用户账户。如果在 RODC 上启用密码缓存，只会影响缓存到本地计算机和用户账户。

④ 只读 DNS。在 RODC 上可以安装 DNS 服务，RODC 可以复制 DNS 使用的所有应用程序目录分区中的数据，包括 ForestDNSZones 和 DomainDNSZones，支持客户端请求 RODC 进行名称解析。在 RODC 上的 DNS 不支持客户端直接更新 DNS 记录，因此 RODC 不会在其拥有的活动目录集成区域内注册任何 NS(Name Server)记录。

⑤ RODC 管理。在可读写的域控制器中，本地管理员和域管理员，都可以管理域控制器。RODC 允许一个普通的域用户成为 RODC 的本地管理员，设置的域用户可以在 RODC 所在的区域执行管理任务，此用户在域中或者任何可读写的域控制器上没有用户权利，仅管理区域分支机构的权限，所以不会影响 Active Directory 整体安全性。

⑥ GC 支持。RODC 可以做 GC 服务器，但是 RODC 不能安装操作主控角色。

(2) RODC 部署要求

如果需要部署 RODC，在网络中必须有一台安装或者升级到的 Windows Server 2008 的域控制器。部署之前，管理员应注意以下事项。

① Active Directory 数据库复制。RODC 支持从 Windows Sever 2003 域控制器复制架构分区和配置分区的数据，但是 RODC 只能从来自同一域的 Windows Server 2008 的可读写域控制器复制域分区的数据更新。因此，在网络中至少安装一台 Windows Server 2008 的域控制器用于 RODC 复制。

② 林功能级别。部署 RODC 需要森林的功能级别最低为 Windows Server 2003 模式，建议使用 Windows Server 2008 模式。用户可以通过在“Active Directory 域和信任关系”窗口中，提升到所需的林功能级别。

③ Windows Server 2008 域控制器的角色为主域控制器，否则将无法识别 RODC 使用的特殊的 Kerberos 票据授权票(KRBTGT)账户。

④ RODC 默认不缓存账户，必须在可读写域控制器上启用账户缓存功能后，才可以用于缓存域用户账户。

⑤ RODC 安装完成后，默认连接的是当前所有的可读写域控制器，必须在 RODC 上，通过“更改域控制器”使其连接到已部署的 RODC 上。

2. 基于服务的 AD DS

默认情况下，可重新启动的 AD DS 在运行 Windows Server 2008 的所有域控制器上都是可用的。使用此功能不存在任何功能级别的要求或任何其他先决条件，与其他服务一样，可以使用 MMC 控制台管理单元或命令行来停止和重新启动 AD DS。需要注意的是，如果停止了 AD DS，则 DNS、KDC 以及站间消息传递服务也会停止。

停止 AD DS 与在目录服务恢复模式中登录 AD DS 相似，但是可重新启动的 AD DS 为运行 Windows Server 2008 的域控制器提供了一种新的状态：AD DS 停止。在此状态下，域控制器与目录服务恢复模式和域成员服务器的特性类似。在目录服务还原模式时，位于本地域控制器上的活动目录数据库(Ntds. dit)处于脱机状态。如果其他域控制器可用，本地域控制器可以使用其进行登录。如果无法联系到其他域控制器，可以使用“目录服务还原

模式密码"登录。作为成员服务器,该服务器被加入域,组策略或者其他设置仍被应用到计算机,但其无法为登录请求服务或者与其他域控制器进行复制操作。

3. 目录数据库

域控制器的任务除了存储 Active Directory 数据库,还负责存储和发布与组策略有关联的文件。Active Directory 域控制器必须支持下级客户端,提供一个存储空间来获取 Config. pol 及 Ntconfig. pol 中包含的本地策略和系统策略。在 Active Directory 域控制器中,存储空间的位置就是 SYSVOL 的共享文件夹,这个文件夹的位置在使用 Dcpromo 提升域控制器期间自动创建。

SYSVOL 必须存储在 NTFS 卷中,因为 SYSVOL 中的文件夹要使用重分析点,而只有 NTFS 格式才支持重分析点。

SYSVOL 包含一个名为 Domain 的文件夹,其中容纳了组策略文件和脚本。组策略文件存储在一个名为 Policies 的子文件夹中,而脚本存储在 Scripts 子文件夹中,Scripts 文件夹作为 NetLogon 来共享,以支持下级客户端。在 SYSVOL 文件夹创建一个文件,在 Domain 文件夹下会立即生成一个新创建的文件的副本。

客户端访问 SYSVOL,必须运行 Dfsclient 服务。域控制器之间 SYSVOL 的内容自动同步,文件复制服务(FRS)就是负责对不同 DC 之间的内容进行同步。

SYSVOL 在服务器上存储网络中使用的特殊资源,删除该共享资源会导致域控制器所服务的所有客户端计算机管理功能丢失。

如果 Active Directory 数据库和 SYSVOL 都安装在同一个磁盘上,由于 Active Directory 数据库系统频繁地响应访问请求,势必会降低系统性能。因此,建议将 SYSVOL 重定位到其他逻辑驱动器或物理驱动器中,以便提升系统性能或者为 SYSVOL 或 FRS 暂存文件夹获取更多的可用磁盘空间。

在规划 Active Directory 时,没有仔细规划 SYSVOL 所在驱动器的存储空间,在网络中应用时发现 SYSVOL 需要的空间不足,可以将 SYSVOL 重新定向到新的网络驱动器中。

FRS 监视 SYSVOL,如果对存储在 SYSVOL 上的任何文件进行更改,那么,FRS 会自动将更改的文件复制到此域中其他域控制器的 SYSVOL 文件夹中。

SYSVOL 每天的工作是自动进行的,除了注意来自监视系统的警报外,不需要任何人为干涉。在更改网络时,可执行一些系统维护操作。

4. 权限委派

委派是 Active Directory 最重要的安全功能之一,用于将某一功能的处理和管理的责任,分配给另一个用户、组或组织单位的权利。通过委派管理,可以为适当的用户和组指派一定范围的管理任务,既可以减少需要具有较高管理权限的管理员用户账户数量,还可以为普通用户和组指派基本管理任务,而让 Domain Admins 和 Enterprise Admins 组的成员执行域范围和林范围的管理。

通过在域中创建组织单位,并将特定组织单位的管理控制权委派给特定用户或组,可将管理控制权委派给域树的任何层次。通常情况下,可以向如下 Active Directory 容器委派管理权限:组织单位、域、站点。

5. 域用户组

组是系统管理和网络管理中的常用功能之一。本地计算机中的组通常只用于管理本地

计算机上的用户账户或组,不支持任何安全设置。域用户组根据其类型和作用域的不同,用途和作用范围也有所不同。

(1) 组类型

创建域组时,在“组类型”选项区域中可选择组的类型。

① 安全组。可以显示在随机访问控制列表(DACL)中的组,该列表用于定义对资源和对象的权限。“安全组”也可用作电子邮件实体,给这种组发送电子邮件的同时也会将该邮件发给组中的所有成员。

② 通讯组。仅用于分发电子邮件并且没有启用安全性的组。不能将“通讯组”显示在用于定义资源和对象权限的随机访问控制列表(DACL)中。“通讯组”只能与电子邮件应用程序(例如,Microsoft Exchange)一起使用,以便将电子邮件发送到用户集合。如果因为安全目的并不需要组,可以选择创建“通讯组”而不要创建“安全组”。

(2) 组作用域

Windows 域中的组作用域包括 3 种:本地域、全局和通用。

本地域组主要用于指定其所属域内的访问权限,以便访问该域内的资源。对于只拥有一个域的企业而言,建议选择“本地域组”。本地域组内的成员可以是任何一个域内的用户、通用组与全局组,也可以是同一个域内的域本地组,但不能是其他域内的域本地组。

全局组主要用于组织用户,即可以将多个被赋予相同权限的用户账户加入到同一个全局组内。全局组内的成员,只能包含所属域内的用户与全局组。全局组可以访问任何一个域内的资源。

通用组可以设置在所有域内的访问权限,以便访问所有域资源。通用组成员可以包括整个域林(多个域)中任何一个域内的用户,但是,无法包含任何一个域内的域本地组。通用组可以访问任何一个域内的资源。

3.3 文件服务安全

文件服务主要用于提供用户所需的文件资源,对于企业网络而言,文件服务器的安全将直接影响业务处理等办公活动的开展。通常情况下,企业内部用户权限过大、登录控制机制疏松,都可能导致内部机密文件被窃取。在 Windows Server 2008 文件服务器上,可以通过文件访问权限、磁盘配额、文件屏蔽等措施,确保文件服务器及重要文件的安全。

3.3.1 NTFS 权限安全配置

NTFS 是目前最安全的文件系统,也是服务器的首选文件系统。Windows Server 2008 要求系统分区文件系统必须为 NTFS,并且由于 NTFS 文件系统能够很好地支持大文件存储和大容量分区,更适合文件服务器的需求。NTFS 文件系统提供了非常严格的访问权限设置,管理员可以为不同类型的用户赋予不同的访问权限,避免由于用户权限过大,而威胁到文件服务器的安全。

1. 设置 NTFS 文件夹和文件权限

(1) 以管理员账户登录系统,打开 Windows 资源管理器,右击欲设置 NTFS 权限的文件夹(本例以 test 文件夹为例),并选择快捷菜单中的“属性”选项,打开“test 属性”对话框,

单击"安全"标签切换至如图 3-41 所示的"安全"选项卡。

(2) 在"组或用户名"列表框中选择想要配置权限的用户账户,如 hstjl,在下面的权限列表框中即可查看其当前权限。单击"编辑"按钮,显示如图 3-42 所示的对话框。继续在"组或用户名"列表框中选择 hstjl,即可在下面的"hstjl 的权限"列表中修改其权限。默认情况下,是没有对普通用户设置任何 NTFS 访问权限的,用户账户将自动继承来自其所属组的权限,文件夹将自动继承来自其父文件夹的 NTFS 权限。

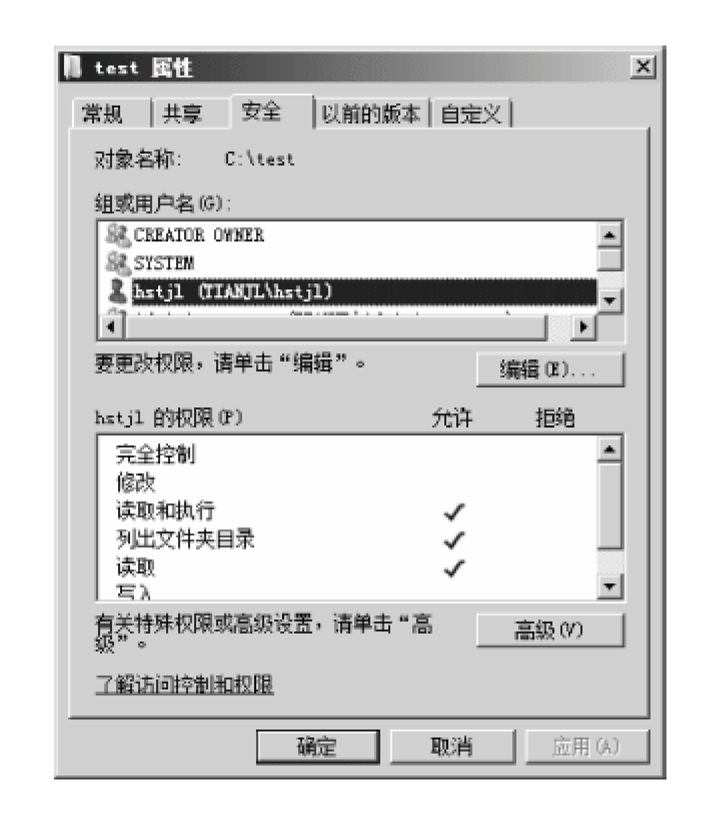


图 3-41 "test 属性"对话框

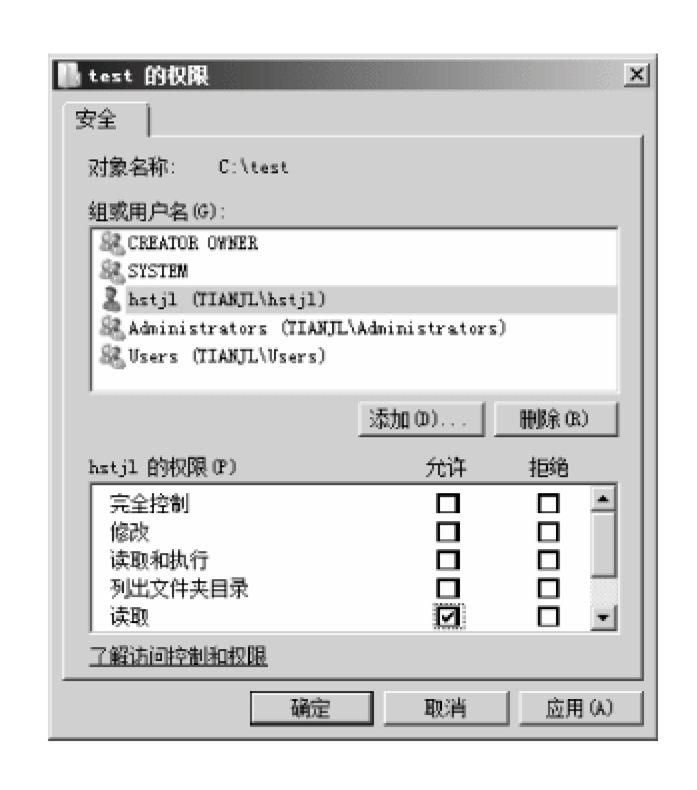


图 3-42 更改用户权限

提示:如果权限带阴影显示,说明这些权限是从父文件夹的权限继承过来的。

(3) 如果"组或用户名"列表框中默认没有需要的用户账户,则可以单击"添加"按钮,显示如图 3-43 所示的"选择用户或组"对话框,在"输入对象名称来选择(示例)"文本框中,输入想要添加的用户账户名并单击"确定"按钮即可。在域控制器上还可以直接添加其他被信任域中的用户账户。



图 3-43 "选择用户或组"对话框

(4) 在"更改用户权限"对话框的"组或用户名称"列表框中,选择想要删除的用户或组,并单击"删除"按钮,即可将其从列表中删除。如果此时该账户所属组未被删除,则该账户仍具有相应访问权限。

(5) 单击"应用"和"确定"按钮,保存设置即可。重复上述操作,可以为不同用户账户指定不同的 NTFS 文件夹权限。

设置 NTFS 文件权限与设置 NTFS 文件夹权限非常相似,如图 3-44 所示,此处不再赘述。NTFS 文件权限仅对目标文件有效,但建议用户尽量不要采用直接为文件设置权限的方式,而是应当将文件放置于文件夹中,然后对该文件夹设置权限。

2. 取消 Everyone 所有权限

Everyone 组是 Windows 系统中的一个特殊组,代表所有当前系统或网络上的所有用户账户,包括来自其他域或网络计算机的来宾账户,并且无论用户何时登录到网络上,或通过网络访问本地计算机,都会自动将该用户添加到 Everyone 组中。如果为 Everyone 组赋予某种控制权限,则任何用户都可以对所涉及的文件夹或文件进行操作,严重影响系统安全,因此建议取消 Everyone 组的所有权限。需要注意的是,在早期版本的 Windows NT 系

统中，匿名登录用户也是属于 Everyone 组的，但在 Windows Server 2003/2008 系统中，“匿名登录”组在默认情况下已不是 Everyone 组的成员。

在资源管理器中，右击磁盘盘符，打开磁盘属性对话框，切换到“安全”选择卡，继续单击“编辑”按钮，显示如图 3-45 所示的对话框，在“组或用户名”列表框中选择 Everyone，并单击“删除”按钮将其删除。最后，单击“确定”按钮保存设置即可。





图 3-44　设置 NTFS 文件权限



图 3-45　删除 Everyone 组

默认情况下，在 Windows Server 2008 系统中，Everyone 组只被赋予了很少的读取权限，安全性已相对较高，但在早期版本的 Windows NT 系统中，该账户却拥有完全控制权限，很容易对系统安全造成威胁。

3.3.2　磁盘配额

如果要在已经使用的磁盘中启用磁盘配额功能，Windows Server 2008 将计算到启动时间点为止，在该卷中复制文件、保存文件或取得文件所有权的所有用户，使用的磁盘空间。根据统计结果，自动为每个用户设置配额限度和警告级别。当然，管理员可以为某个或多个用户设置不同的配额或禁用配额。另外，也可以为还没有在卷上复制文件、保存文件和取得文件所有权的用户设置磁盘配额，或者在一个新创建的卷上启用磁盘配额功能。

1. 启动磁盘限额

在默认的情况下，磁盘配额是没有启用的。启动磁盘配额的操作步骤如下。

（1）在 Windows 资源管理器中，右击想要启用配额功能的 NTFS 卷（如本地磁盘 C），并选择快捷菜单中的“属性”选项，打开“本地磁盘（C:）属性”对话框，切换到如图 3-46 所示的“配额”选项卡，选中“启用配额管理”复选框，即可启用磁盘配额管理。

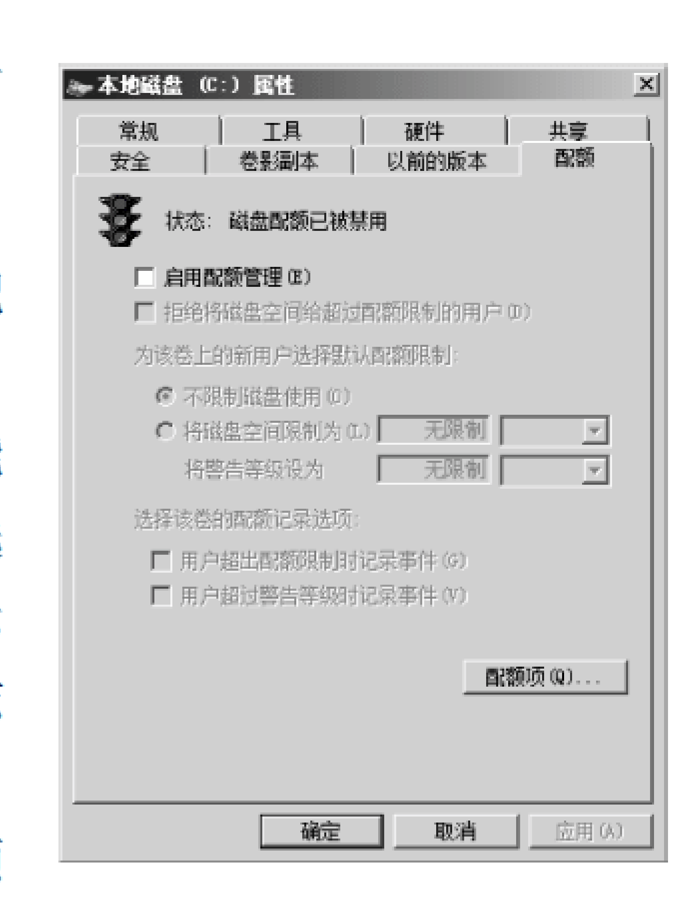


图 3-46　“配额”选项卡

选择其中相应的各个选项，以配置系统的磁盘配额功能。

① 选中“拒绝将磁盘空间给超过配额限制的用户”复选框，超过其配额限制的用户，将收到来自 Windows 的“磁盘空间不足”的错误信息，并且在没有从中删除和移动一些现存文件的情况下，无法将额外的数据写入卷中。如果清除该复选框，则用户可以超过其配额限制。

② 选中“将磁盘空间限制为”单选按钮，并输入允许卷的新用户使用的磁盘空间数量，以及在将事件写入系统日志前已经使用的磁盘空间量。网络管理员可以在“事件查看器”中查看这些事件。在磁盘空间和警告级别中可以使用十进制数值，从下拉列表框中选择适当的单位（如 KB、MB、GB 等）。

③ 选中“用户超出配额限制时记录事件”复选框。此时如果启用配额，则只要用户超过其配额限制，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

④ 选中“用户超过警告等级时记录事件”复选框。此时如果启用配额，则只要用户超过其警告级别，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

（2）单击“确定”按钮，保存所做设置，启用磁盘配额完成。

（3）启用磁盘配额管理后，所有的用户都使用磁盘配额启动时设置的默认配额限制和配额警告级别。使用配额项目管理可以为每一个用户设置适合的磁盘配额，对用户的磁盘配额设置进行维护，并且可以记录每一个用户对磁盘空间的使用情况。

2．为特定的用户磁盘配额

若想让某一个用户使用更多的空间，可以为该用户单独制定更大的磁盘配额。

（1）在“驱动器属性”对话框中，选择“配额”选项卡，单击“配额项”按钮，显示如图 3-47 所示的“（D:）的配额项”窗口。

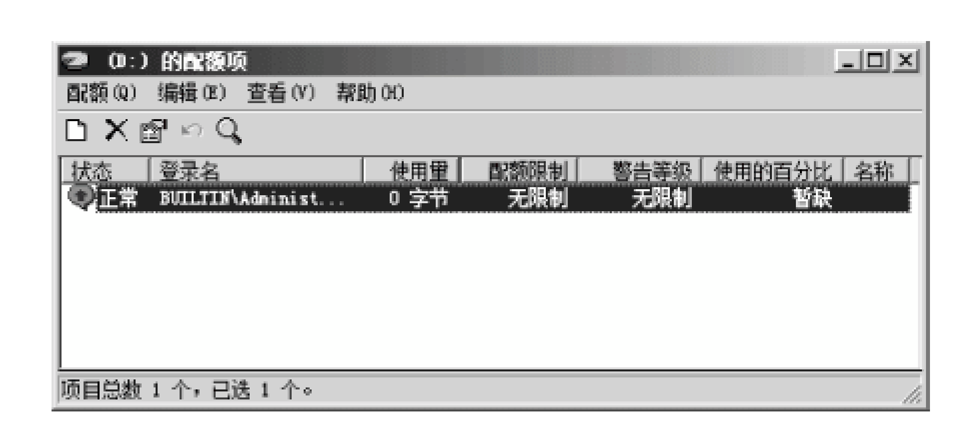


图 3-47 “（D:）的配额项”窗口

（2）选择“配额”下拉菜单中的“新建配额项”选项，或者单击工具栏中的“新建配额项”图标按钮，显示如图 3-48 所示的“选择用户”对话框。在“选择此对象类型”文本框中显示出当前的对象类型为用户，可采用系统的默认值。在“输入对象名称来选择（示例）”文本框中，输入要设置配额的用户名称。单击“检查名称”按钮，检查输入的用户账户是否存在。

（3）单击“确定”按钮，显示如图 3-49 所示的“添加新配额项”对话框。选中“将磁盘空间限制为”单选按钮，并在其后文本框中为该用户设置访问磁盘的空间。



图 3-48 “选择用户”对话框

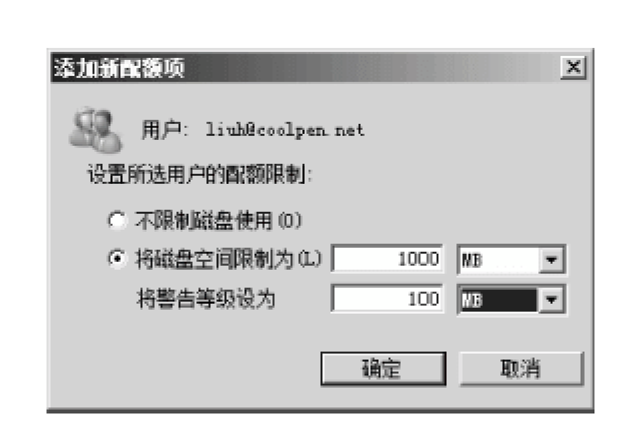


图 3-49 “添加新配额项”对话框

（4）单击“确定”按钮，保存用户的磁盘配额设置，返回到“（D:）的配额项”窗口，可以看到新创建的用户“刘红”配额项显示在列表框中。

如果想删除指定用户的配额项，可选择用户名，右击并选择快捷菜单中的“删除”选项即可。

使用指定配额项具有以下优点。

（1）登录到相同计算机的多个用户之间互不影响。

（2）一个或多个用户不独占公用服务器上的磁盘空间。

（3）在个人计算机的共享文件夹中，用户不会使用过多的磁盘空间。

3. 监控每个用户的磁盘配额使用情况

当为用户设置好磁盘配额以后，除了可以借助“日志查看器”浏览磁盘占用情况外，在配额项窗口中，也可以监视每个用户的磁盘配额使用情况，并可单独设置每个用户可使用的磁盘空间。也就是说配额项的主界面就是一个用户配额监控器。

若欲更改某一个用户的磁盘配额设置，可右击该用户，选择快捷菜单中的“属性”选项，显示如图 3-50 所示的“刘红（liuh@coolpen. net）的配额设置”对话框，可以更改用户的磁盘空间限制及警告等级。

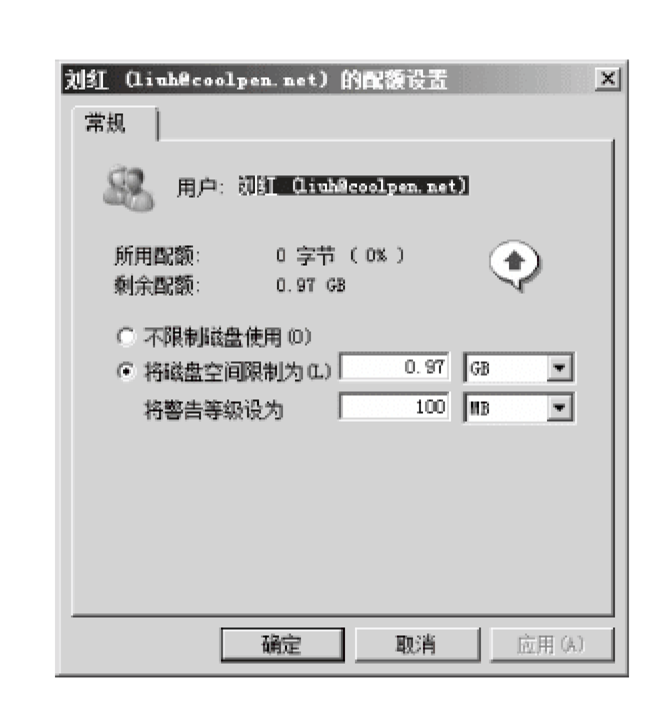


图 3-50 “刘红（liuh@coolpen. net）的配额设置”对话框

3.3.3 文件屏蔽

文件屏蔽是文件服务器中的重要功能，部署文件服务器之后，即可使用该功能限制用户向文件服务器写入的文件类型。任何用户将限制类型的文件写入目标文件夹时，将出现“目标文件夹访问被拒绝”的被拒绝信息。文件屏蔽的主要目的是限制非法授权文件写入定义的文件夹。

1. 安装文件服务器资源管理器

文件屏蔽是文件服务器的可选功能之一，用户可以根据需求选择安装。如果安装文件服务器的同时，在“选择角色服务”列表中选中了“文件服务器资源管理器”角色服务，则可以直接配置文件屏蔽和应用。如果没有安装，则可以通过“添加角色服务”向导再次添加相应角色服务，操作步骤如下。

（1）在“服务器管理器”窗口中，找到已经安装好的“文件服务器”，单击“添加角色服务”链接，启动“添加角色服务”向导，显示如图 3-51 所示的“选择角色服务”对话框。在“角色服务”列表中选中“文件服务器资源管理器”复选框。

（2）单击“下一步”按钮，显示如图 3-52 所示的“配置存储使用情况监视”对话框，选择希望监视的卷。默认情况下，生成的监视报告中只包括“按所有者的文件报告”和“按文件组的文件报告”两项，单击“选项”按钮，在“卷监视选项”对话框的“报告”列表框中，可以选择希望监视的项目。

（3）单击“下一步”按钮，显示“设置报告选项”对话框。保存报告的默认位置是 C:\StorageReports，用户也可以单击“浏览”按钮自定义。单击“下一步”按钮，显示如图 3-53 所示的“确认安装选择”对话框。如果确认无误，单击“安装”按钮即可开始安装。

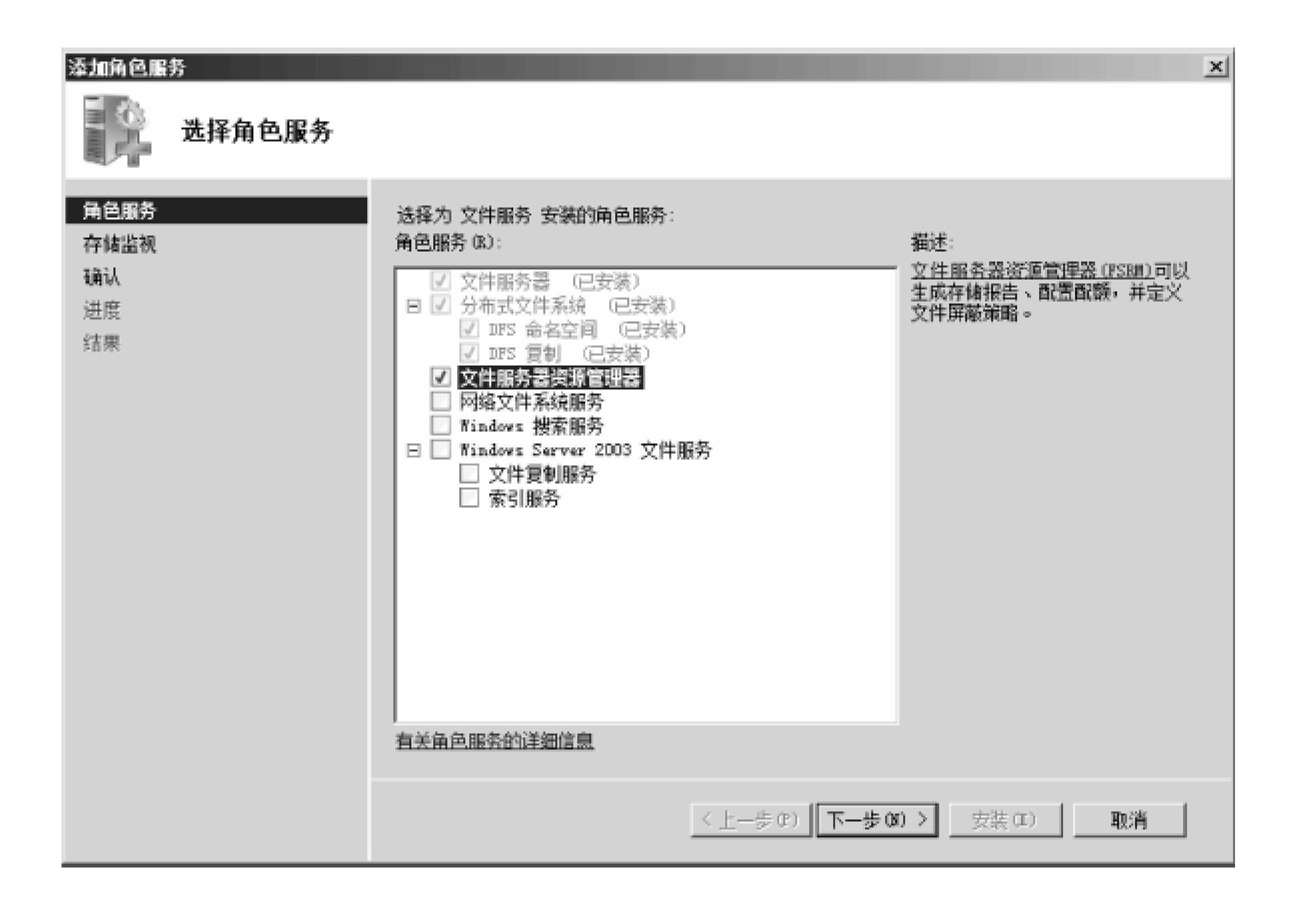


图 3-51 “选择角色服务”对话框

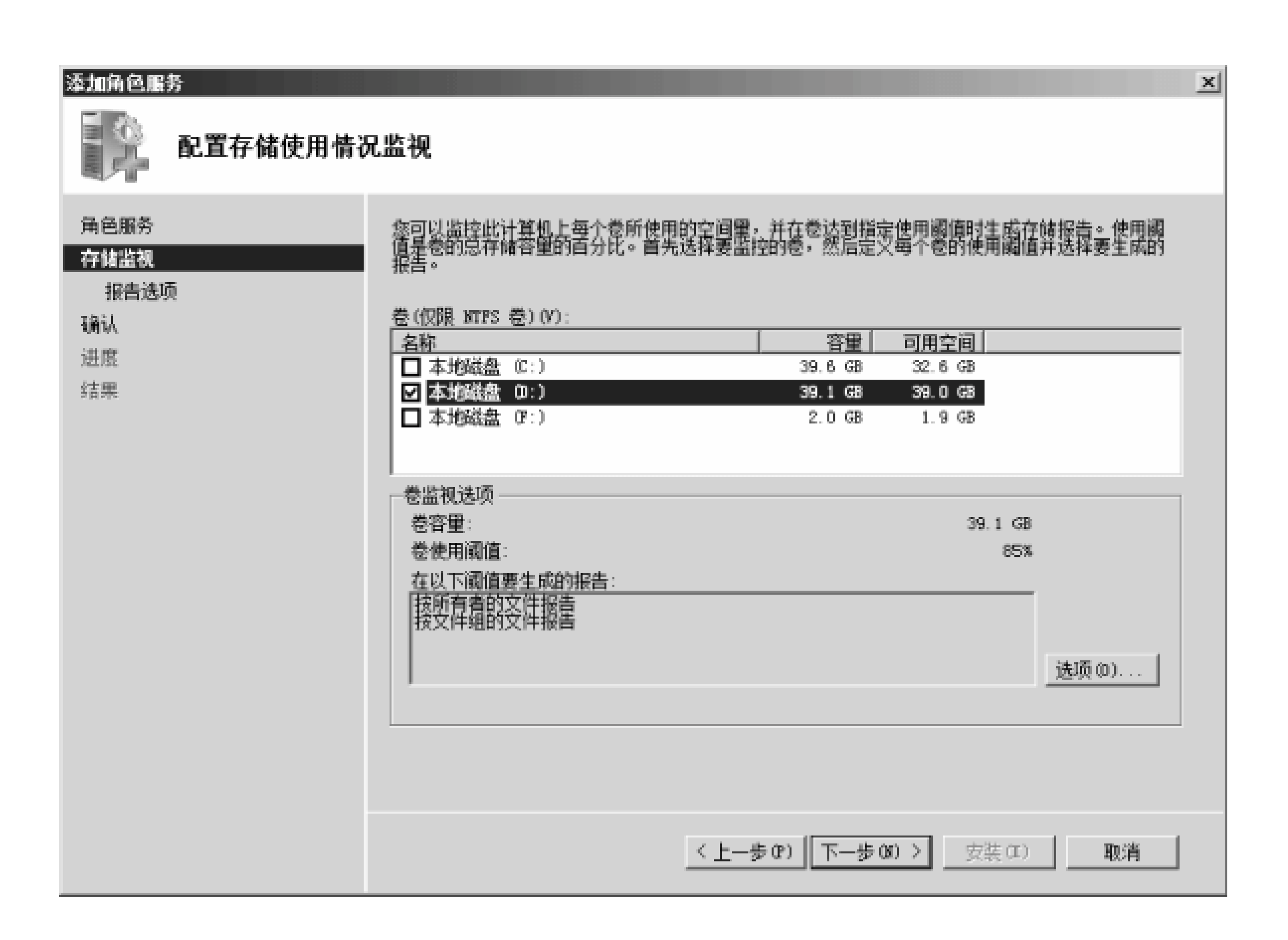


图 3-52 “配置存储使用情况监视”对话框

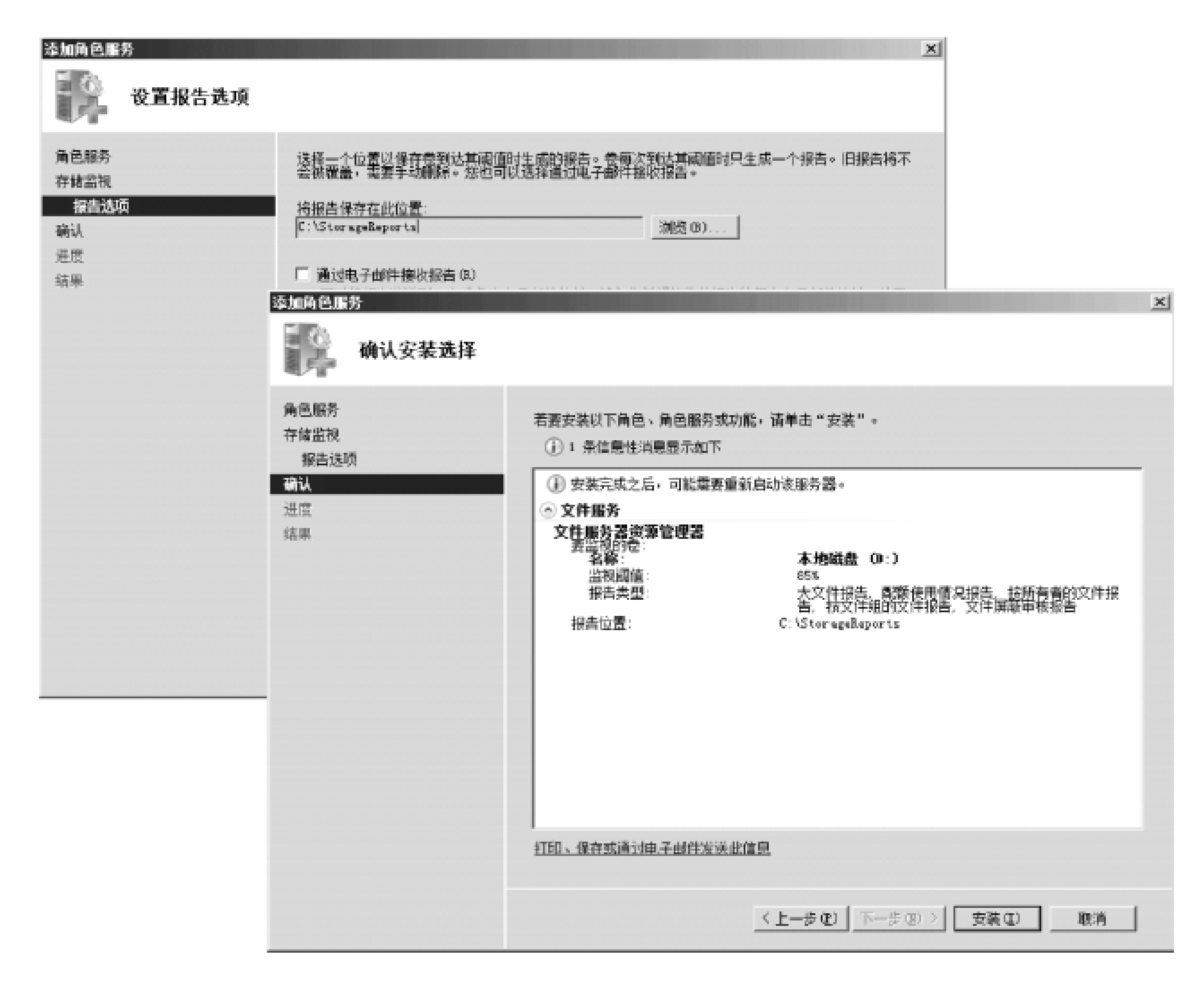


图 3-53 “确认安装选择”对话框

(4) 安装完成后,单击"关闭"按钮退出向导即可。

2. 创建限制文件组

限制文件组,就是定义需要限制的文件类型,支持通配符(* 和? 等)定义。文件服务安装完成后,预定义了 11 个文件组。本例屏蔽除文本文件外的所有文件类型。

(1) 依次选择"开始"→"管理工具"→"文件服务器资源管理器"选项,打开"文件服务器资源管理器"窗口,依次展开"文件屏蔽管理"→"文件组"选项,显示如图 3-54 所示窗口。

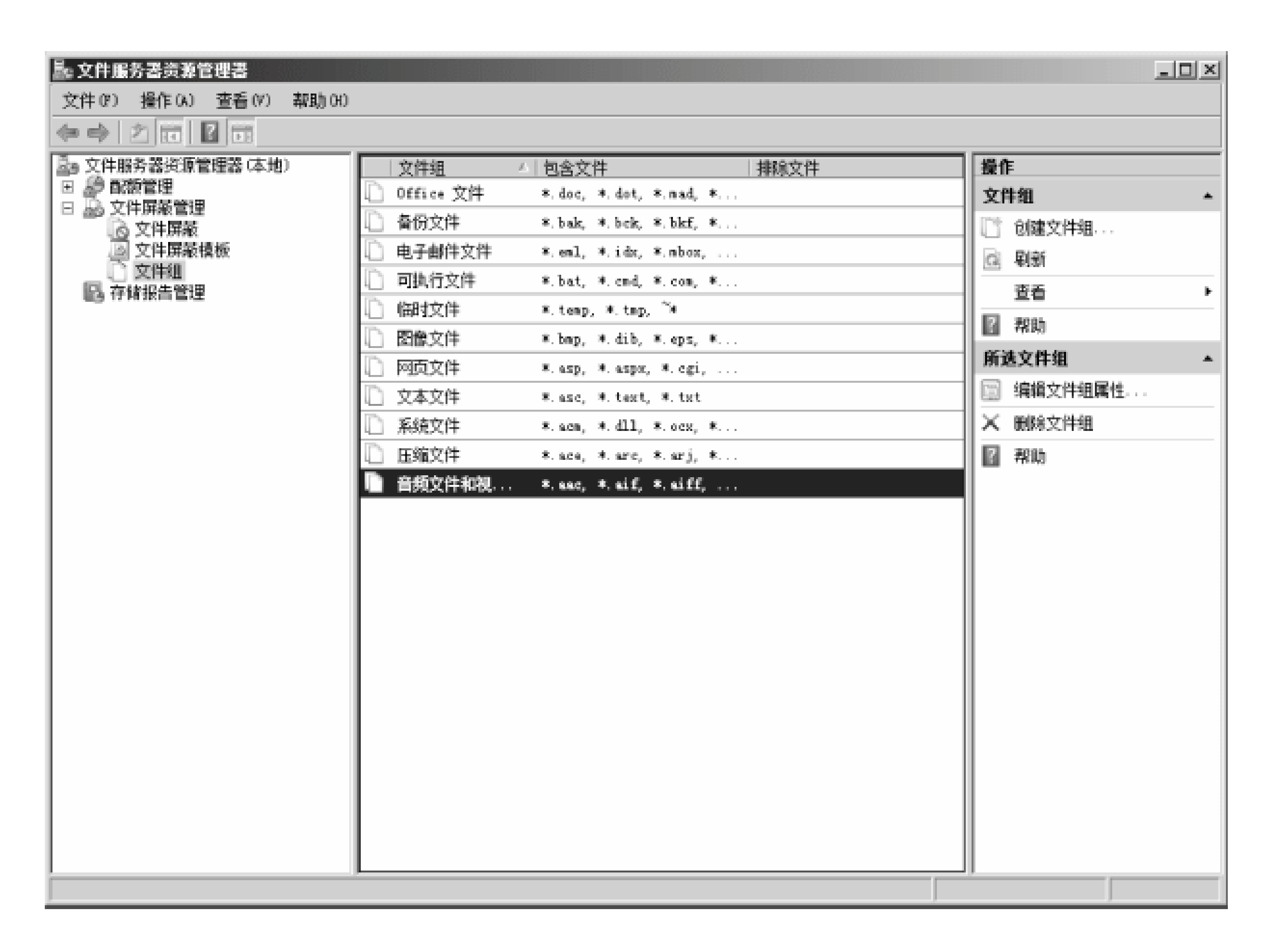


图 3-54　"文件服务器资源管理器"窗口

(2) 右击"文件组",在弹出的快捷菜单中选择"创建文件组"选项,显示如图 3-55 所示的"创建文件组属性"对话框。在"文件组名"文本框中,输入新文件组的名称;在"要包含的文件"文本框中输入"*.*",表示当前策略关联所有类型的文件。

(3) 单击"添加"按钮,将"*.*"加入到文件列表中。如需排除某种类型的文件,可以在"要排除的文件"文本框中,输入对应文件的扩展名(如 *.txt),然后单击"添加"按钮,将其加入到文件列表中,如图 3-56 所示。



图 3-55　"创建文件组属性"对话框(1)

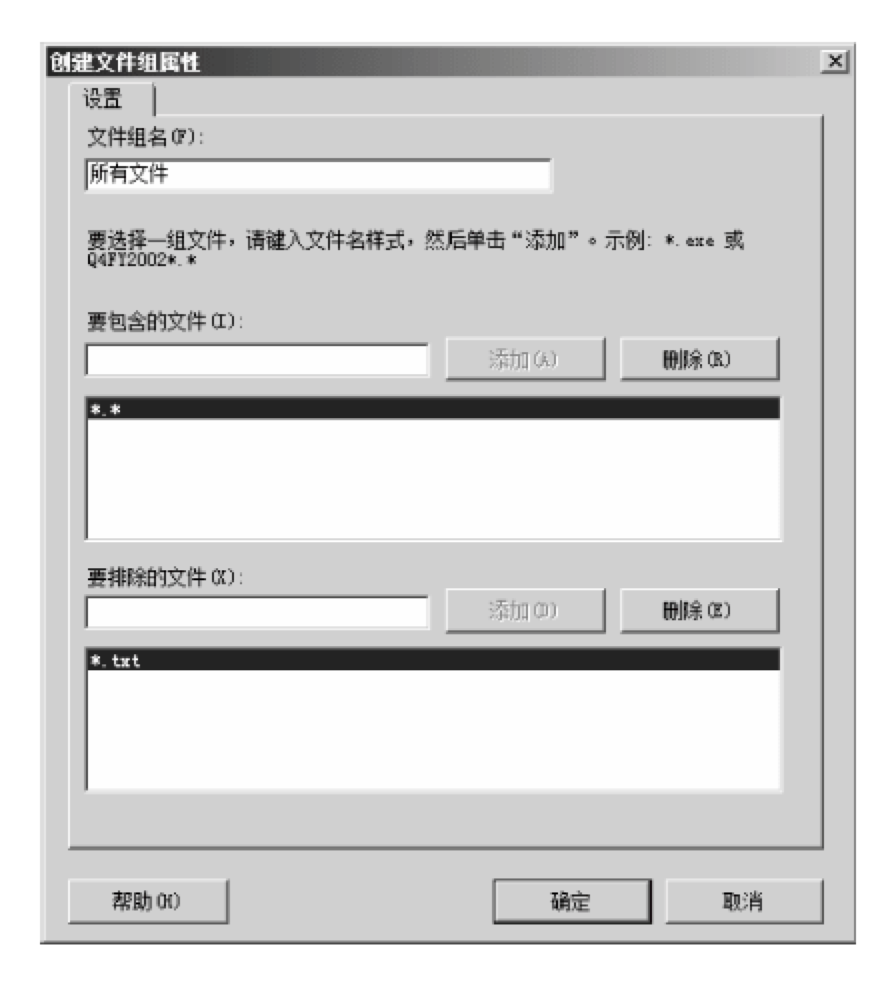


图 3-56　"创建文件组属性"对话框(2)

(4) 单击“确定”按钮，完成新文件组的创建。

3. 创建屏蔽模板

屏蔽模板，定义文件组被监控以及监控方式，提供主动屏蔽和被动屏蔽两种模式。主动屏蔽，将屏蔽文件组中定义的文件类型关联的文件；被动屏蔽，仅监控文件组中定义的文件，但不限制写入目标文件夹。

(1) 在“文件服务器资源管理器”窗口中，展开如图 3-57 所示的“文件屏蔽模板”选项。文件服务安装完成后，默认已经预定义了 5 个文件屏蔽模板。



图 3-57 “文件屏蔽模板”选项

(2) 右击“文件屏蔽模板”，选择快捷菜单中的“创建文件屏蔽模板”选项，显示如图 3-58 所示的“创建文件屏蔽模板”对话框。在“模板名”文本框中，输入新模板的名称；选



图 3-58 “创建文件屏蔽模板”对话框

中“主动屏蔽：不允许用户保存未经授权的文件”单选按钮；在“选择要阻止的文件组”列表框中，选择需要主动屏蔽的文件组，本例中选择新创建的“所有文件”文件组。

提示：“主动屏蔽”和“被动屏蔽”的主要区别在于：“主动屏蔽”屏蔽符合文件组设置的所有文件，“被动屏蔽”监控用户保存到目标文件夹的文件，可以正常写入，仅提供报警功能。

(3) 单击“确定”按钮，显示如图 3-59 所示的“更新从模板派生的文件屏蔽”对话框，选中“仅将模板应用于与原始模板匹配的派生文件屏蔽”单选按钮。

(4) 单击“确定”按钮，完成屏蔽模板的创建。

4. 部署文件屏蔽策略

部署文件屏蔽策略的方法很简单，选择目标文件夹后，将创建的文件屏蔽模板绑定到目标文件夹即可。

(1) 在“文件服务器资源管理器”窗口中，右击“文件屏蔽”并选择快捷菜单中的“创建文件屏蔽”选项，显示如图 3-60 所示的“创建文件屏蔽”对话框。单击“浏览”按钮，选择需要保护的目标文件夹。

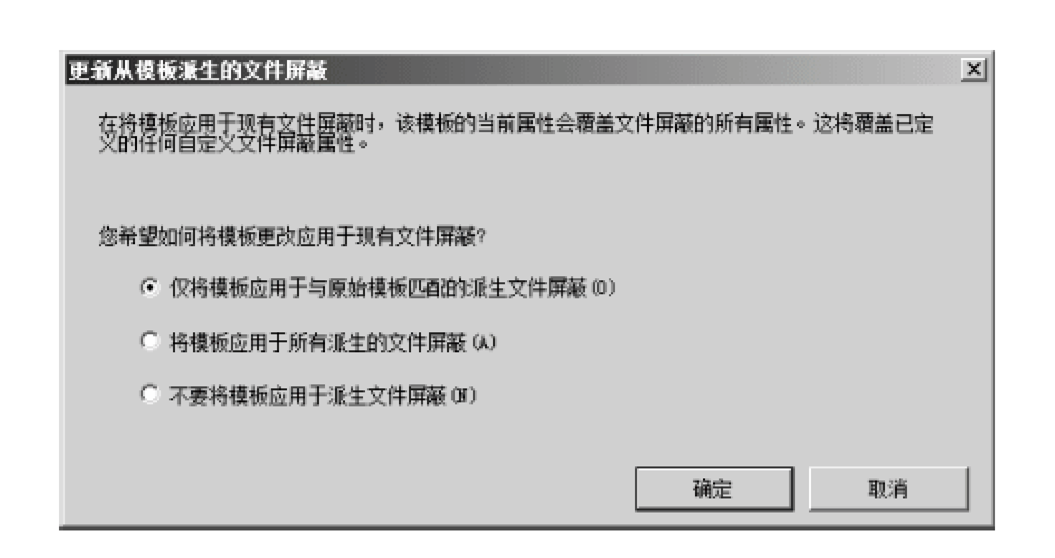


图 3-59　“更新从模板派生的文件屏蔽”对话框

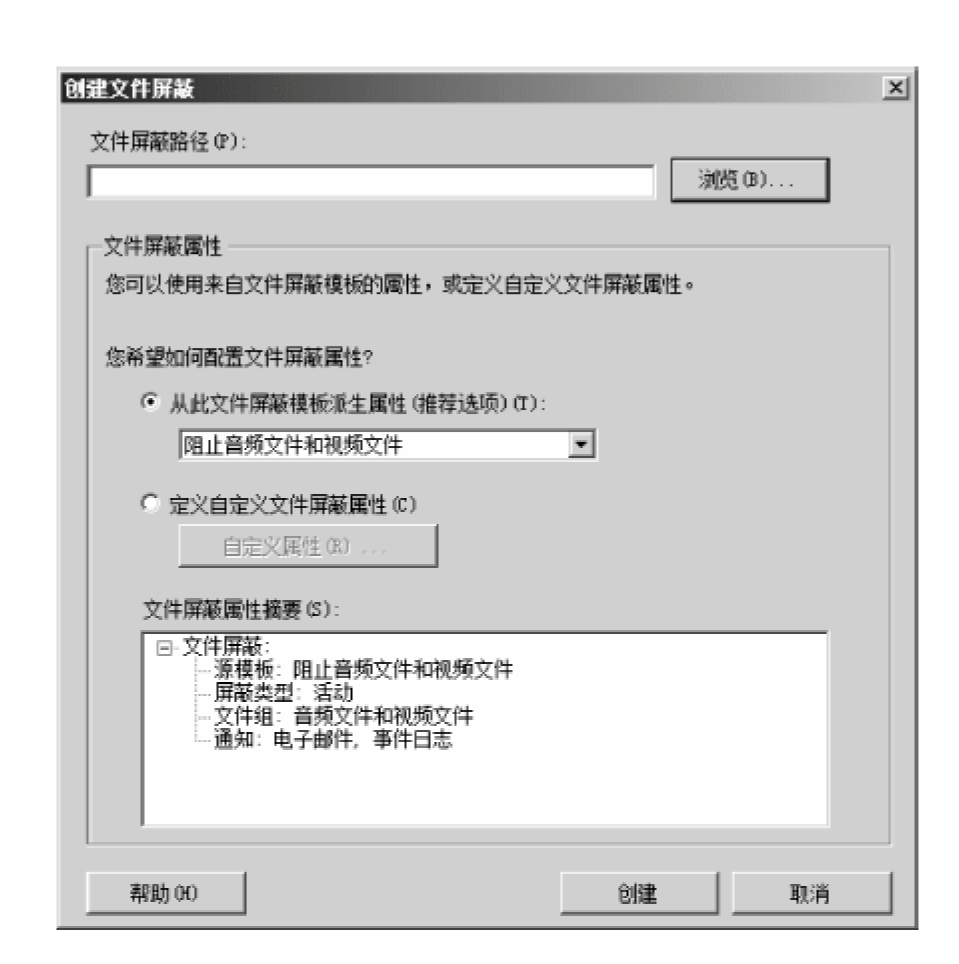


图 3-60　“创建文件屏蔽”对话框

(2) 单击“确定”按钮，返回到“创建文件屏蔽”对话框。在“文件屏蔽属性”选项区域的“从此文件屏蔽模板派生属性(推荐选项)”下拉列表框中，选择“阻止写入文本文件之外的所有文件”选项，在“文件屏蔽属性摘要”列表框中即可显示该屏蔽模板的详细信息，如图 3-61 所示。

(3) 单击“创建”按钮，即可成功创建新的文件屏蔽策略。

5. 文件屏蔽测试

此时文件屏蔽模板的内容是：阻止写入文本文件之外的所有文件。为了验证设置是否生效，可以进行如下实验。

(1) 在受保护的目录下(本例中为 D:\)，新建一个.docx 文件时，显示如图 3-62 所示的“目标文件夹访问被拒绝”对话框，.docx 类型的文档不能被创建。

(2) 仍在该目录下，新建一个.txt 文件时，可以顺利完成，如图 3-63 所示。这是因为屏蔽文件类型中已经排除了.txt 文件。

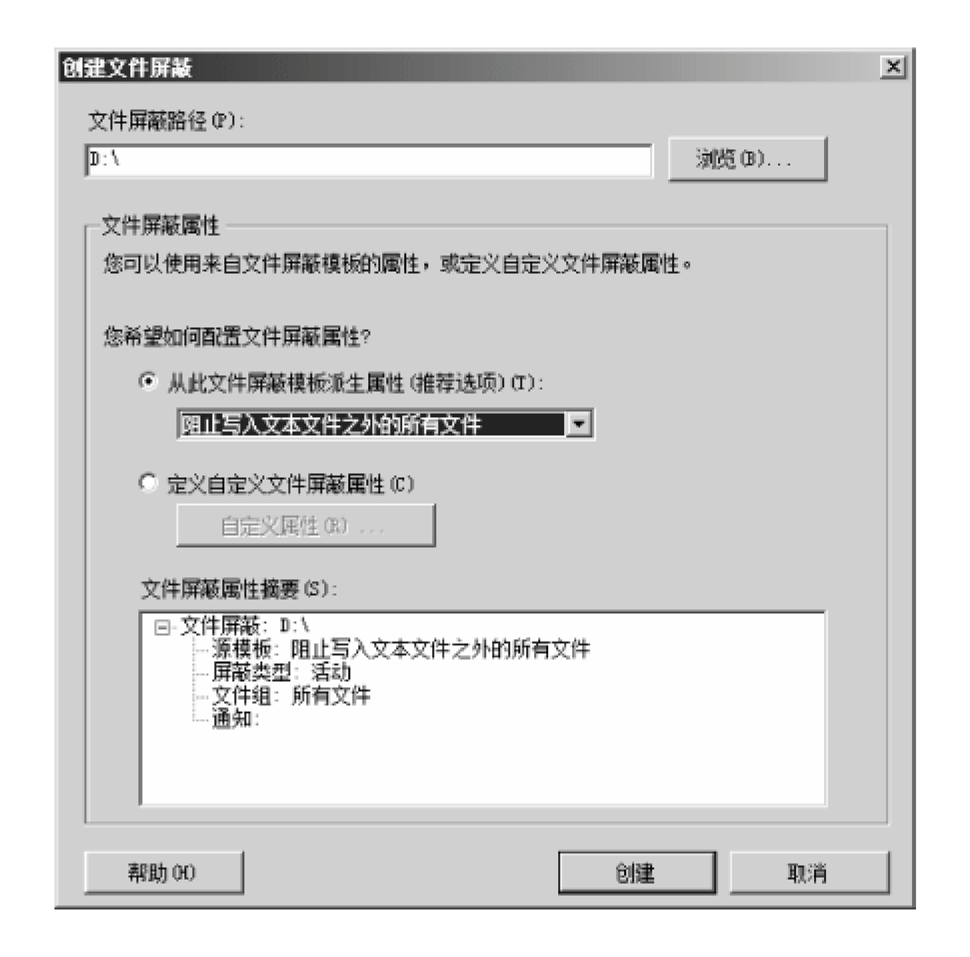


图 3-61 只允许写入文本文件



图 3-62 “目标文件夹访问被拒绝”对话框

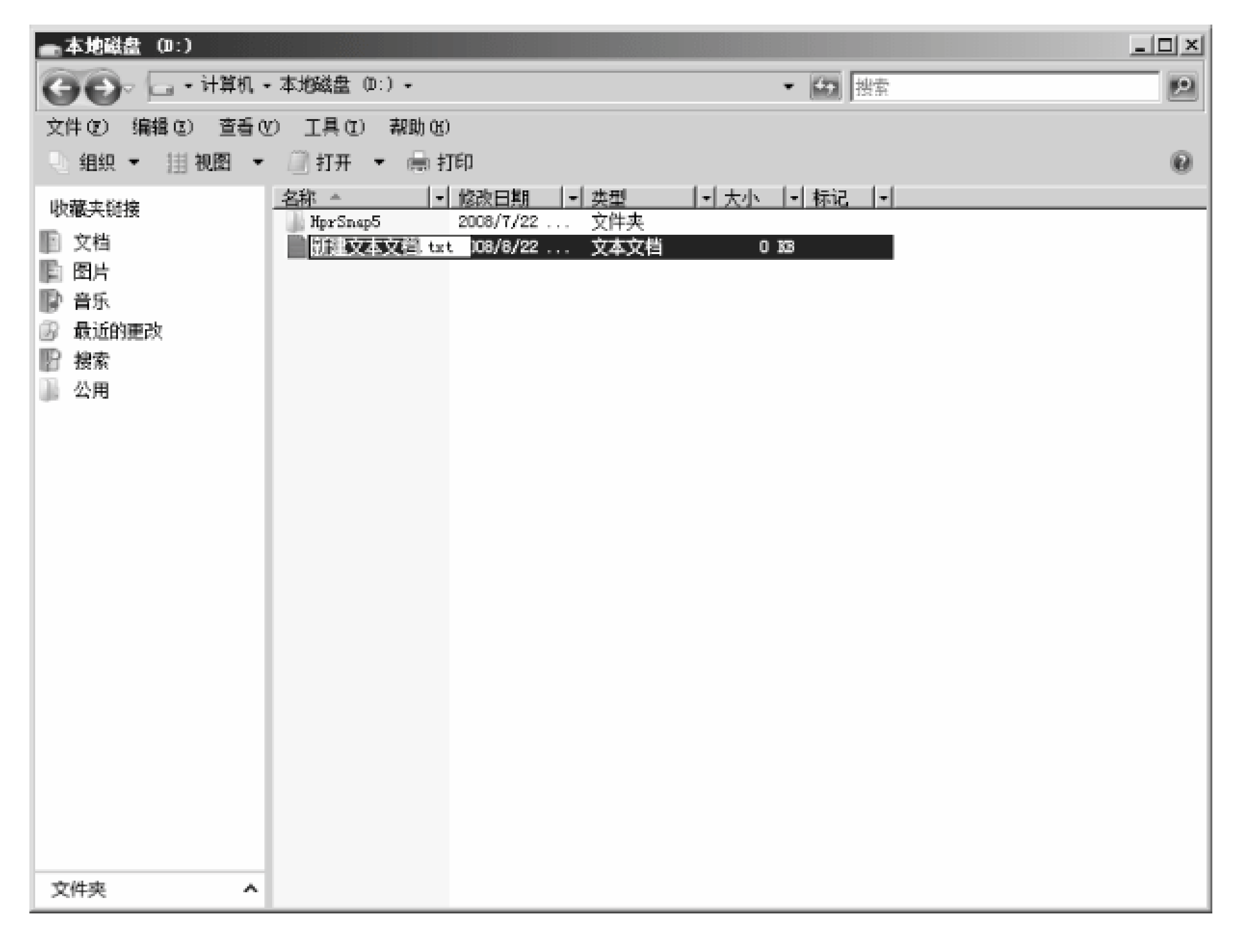


图 3-63 创建测试文本文件

3.3.4 知识链接：文件服务安全

1. 基于 NTFS 文件系统的访问控制

(1) NTFS 文件和文件夹权限

对于 NTFS 分区上的文件和文件夹，管理员可以通过 NTFS 权限限制不同用户账户的访问权限。文件和文件夹的 NTFS 权限有两种类型：显式权限和继承权限。其中，显式权限是系统创建对象时，默认赋予用户账户的访问和操作权限；继承权限是从父对象传播到当前对象的权限。继承权限可以减轻管理权限的任务，并且确保给定容器内所有对象之间的权限一致性。默认情况下，文件将自动继承来自其父文件夹的 NTFS 权限设置。

NTFS 文件夹权限及允许用户完成的操作如表 3-1 所示。

表 3-1 NTFS 文件夹权限及允许用户完成的操作

NTFS 文件夹权限	允许用户完成的操作
读取	查看该文件夹中的文件和子文件夹。查看文件夹的所有者、权限和属性(如只读、隐藏、存档和系统)
写入	在该文件夹内新建文件和子文件夹。更改文件夹属性,查看文件夹的所有者和权限
列出文件夹目录	查看该文件夹中的文件和子文件夹的名称
读取及运行	完成"读取"权限和"列文件夹目录"权限所允许的操作。漫游各个文件夹,以便访问其他文件和文件夹,即使该用户没有访问那些文件夹的权限
修改	完成"写入"权限及"读取及执行"权限所允许的操作。删除文件夹
完全控制	完成其他所有 NTFS 权限允许的操作。更改权限,取得所有权和删除子文件夹和文件

NTFS 文件权限及允许用户完成的操作如表 3-2 所示。

表 3-2 NTFS 文件权限及允许用户完成的操作

NTFS 文件权限	允许用户完成的操作
读取	读该文件和查看文件属性、所有者及权限
写入	覆盖该文件,更改文件属性和查看文件的所有者和权限
读取及运行	完成"读取"权限所允许的操作。运行应用程序
修改	完成"写入"权限和"读取及运行"权限所允许的操作。修改和删除文件
完全控制	完成其他所有 NTFS 文件权限所允许的操作。更改权限和取得所有权

(2) 多重 NTFS 权限

管理员可以根据需要为 NTFS 分区上的文件和文件夹同时设置 NTFS 权限,而文件夹和文件又有可能是包含与被包含的关系,所以必然会产生资源权限的重复,从而直接导致文件夹或文件最终的 NTFS 权限并非是管理员真正需要的结果。

① 权限累积。用户对一个资源的最终权限,是为该用户指定的全部 NTFS 权限和为该用户所属组指定的全部 NTFS 权限之和。如果某用户拥有一个文件夹的读取权限,同时又是对该文件夹有写入权限的用户组的成员,则最终该用户对这个文件夹既有读取权限,也有写入权限。

② 文件权限优先于文件夹权限。NTFS 文件权限优先于 NTFS 文件夹权限,即用户只要有访问一个文件的权限,即使没有访问该文件所在文件夹的权限,也可以访问该文件。

③ 拒绝权限优先于其他权限。在 Windows 系统的所有 NTFS 权限中,拒绝权限优先于其他任何权限。即使用户作为一个组的成员有权访问文件或文件夹,一旦该用户被设置了拒绝访问权限,则最终将剥夺该用户可能拥有的任何其他权限。在实际使用中,应当尽量避免使用拒绝权限。

(3) NTFS 权限的继承性

NTFS 权限是具有继承性的。所谓继承性,就是指 NTFS 权限自动从父对象传播到当前对象的过程,例如子文件夹继承来自其父文件夹的 NTFS 权限,文件继承来自文件夹的

NTFS 权限等。当然，正是因为 Windows 系统默认启用了 NTFS 权限继承，才会使用户不容易更加直观地判断对象最终的 NTFS 权限值。管理员可以根据实际情况，限制这种权限继承。

（4）设置 NTFS 权限基本策略和规则

NTFS 权限不仅在本地系统或本地域中有效，当目标资源在网络上共享时，这些权限设置同样有效，并且优先级高于共享权限设置。因此，从网络安全角度考虑，将资源设置为共享之前，应先配置其 NTFS 权限，以确保访问的安全性。在设置 NTFS 权限时，必须遵循以下基本策略和规则。

① 为了简化管理，应事先对目标文件进行分类管理，将同一类别归于同一文件夹中，例如可以分为应用程序、数据和主目录文件夹等，并将主目录和公共文件夹集中在一个与应用程序和操作系统分开的独立卷上，从而只需为文件夹指定权限，而不必为单独的文件指定权限。另外，将所有历史数据保存在同一目录下，还减少了备份工作的复杂性。

② 在文件夹级指定需要的全部权限，而不是在文件级指定权限。对于希望限制用户访问的文件用单独的文件夹将文件分组，然后为该文件夹指定受限制的访问权限。

③ 只允许用户拥有他们所需要的存取级别，也就是说，为用户或用户组指定最严格的 NTFS 权限，只要能够完成所需的任务即可，从而减少用户意外修改或删除重要文档和程序文件的可能性。如果用户只需要读取一个文件，那么，就只赋予其对该文件的读取权限。

④ 按照组成员对资源的访问需要创建组，然后，为组指定适当的权限。只有必要时才为单独的用户指定权限。

⑤ 对于全部应用程序的可执行文件，应当为 Administrators 组指定读取、执行权限和更改权限，但只为 Users 组指定读取和执行权限，从而有效防止应用程序文件被删除或破坏。

⑥ 对于公共数据文件夹，应当为 Creator Owner 指定完全控制权限，使用户可以删除和修改其创建的文件和文件夹，从而完全访问在公共数据文件夹中创建的文件或文件夹。

⑦ 对于公共文件夹，应当为 Everyone 组指定读取权限和写入权限，并为 Creator Owner 指定完全控制权限，使用户能够完全访问他们创建的文件，读取和修改其他用户创建的文件，并能够读取、修改和删除他们自己创建的文件和文件夹。同时，Everyone 组的成员只能读取该文件夹中的文件，并可向该文件夹中添加文件。

⑧ 设置允许权限而不是拒绝权限。如果不希望让某个用户或用户组访问某个特定的文件夹或文件，就不要为其指定权限。拒绝权限应当是个例外，而不是经常使用的操作。只有在必须拒绝特定的用户账户或组的某种特定的访问类型时，才设置拒绝权限。

⑨ 如果只是在这台计算机上访问资源，则使用描述性的长文件名。如果该文件夹将来要共享，则使用可被所有客户计算机访问的文件夹和文件名，建议采用短文件名的格式。

借助于文件服务器中设置的访问控制列表（ACL），不仅可以最大限度地保障重要数据存储安全，保证数据不会由于计算机的硬件故障而丢失，而且还可以通过严格的权限设置，有效地保证数据的访问安全。

网络攻击的目的在于获取用户权限，而获取用户权限的目的，在于获取超级文件权限。因此，做好文件权限的访问控制，才是最重要和最有效的安全措施。

（5）复制和移动文件夹对权限的影响

在 NTFS 分区内和 NTFS 分区之间复制或者移动文件、文件夹时，Windows 系统会将

其作为新文件或文件夹，因此，会对源文件或文件夹的 NTFS 权限产生影响。在复制文件和文件夹时，必须拥有源文件夹的“读取”权限，并且对目标文件夹具有“写入”权限。在移动文件或文件夹时，必须对目标文件夹拥有“写入”权限，并且对源文件夹拥有“修改”权限。

当从一个文件夹向另一个文件夹复制文件或文件夹时，或者从一个磁盘分区向另一个磁盘分区复制文件或文件夹时，复制文件或文件夹对 NTFS 权限产生下述影响。

① 当在单个 NTFS 分区内复制文件夹或文件时，文件夹或文件的复制将继承目的文件夹的权限。

② 当在 NTFS 分区之间复制文件夹或文件时，文件夹或文件的复件将继承目的地文件夹的权限。

③ 当将文件或文件夹复制到非 NTFS 分区时，因为目标分区不再支持 NTFS 权限，所以，这些文件或文件夹将丢失 NTFS 权限。

移动对 NTFS 权限的影响如下。

① 当在单个 NTFS 分区内移动文件夹或文件时，该文件夹或文件保留其原来的权限。

② 当在 NTFS 分区之间移动文件夹或文件时，该文件夹或文件将继承目的地文件夹权限。当在 NTFS 分区之间移动文件夹或文件时，实际是将该文件夹或文件复制到新位置，然后，将其从原来的位置删除。

③ 当将文件或文件夹移动到非 NTFS 分区时，因为非 NTFS 分区不支持 NTFS 权限，所以，这些文件和文件夹将丢失其 NTFS 权限。

2. 磁盘配额

磁盘配额是 NTFS 文件系统特有的安全功能，可以帮助管理员控制每个用户账户的磁盘空间使用情况。磁盘配额是以文件所有权为基础的，只应用于卷，且不受卷的文件夹结构及物理磁盘上的布局影响。由于磁盘配额监视个人用户卷的使用情况，因此，每个用户对磁盘空间的利用都不会影响同一卷上其他用户的磁盘配额。

磁盘配额管理技术，主要是根据网络管理员设置的标准，跟踪对被保护卷的写操作，如果被保护卷达到或超过了设定级别，则用户就会收到服务器自动发送的消息，警告该卷已经接近配额，或者磁盘配额管理器将阻止用户向该卷写数据。管理员能够启用磁盘配额，并设置两个值。

（1）磁盘配额限度。用于指定允许用户使用的磁盘空间容量。

（2）磁盘配额警告级别。指定了用户接近其配额限度的值。

使用磁盘配额过程中，应注意如下 3 个方面。

（1）驱动器的文件格式必须为 NTFS 文件系统格式。如果驱动器的磁盘格式为 FAT32 文件系统，可以使用 Windows Server 2003/2008 提供的文件系统转换工具 Convert 进行转换。

（2）必须以管理员或管理员组成员的身份登录到 Windows 系统。

（3）在文件服务器上选中“为此服务器的新用户设置默认磁盘空间配额”复选框，在“将磁盘空间限制为”和“将警告级别设置为”文本框中，输入适当的数值，使用户只能使用规定数额的磁盘空间，从而避免服务器硬盘的滥用。当用户使用的空间达到指定的警告值时，系统将提示用户磁盘空间剩余值。当用户使用的空间达到规定的磁盘限额时，系统将禁止用户再向服务器写入文件，从而确保服务器硬盘空间被合理、公平地使用。

3. 文件屏蔽

在文件服务器资源管理器的“文件屏蔽管理”中,可以执行下列任务。

(1) 通过创建文件屏蔽来控制用户可以保存的文件类型,以及在用户尝试保存未经授权的文件时生成通知。

(2) 定义可以应用于新的卷或文件夹,以及可以在整个组织中使用的文件屏蔽模板。

(3) 创建增强文件屏蔽规则灵活性的文件屏蔽例外。

(4) 确保服务器上的个人文件夹中未存储任何音乐文件,还可以允许存储支持法律权限管理或符合公司策略的特定媒体文件类型。

(5) 执行屏蔽进程,在共享文件夹中存储可执行文件时通过电子邮件通知用户,其中包含存储文件的用户和文件的准确位置等信息,以使用户可以采取相应的预防措施。

3.4 IIS 服务安全

IIS 是 Windows 系统中最常用的网络服务之一,可以为 Internet 或 Intranet 提供 WWW 服务和 FTP 服务。不仅如此,许多网络服务也是基于 IIS 服务的,例如流媒体服务、终端服务等。如何加强 IIS 的安全机制,建立高安全性能的可靠的 WWW 服务器,已成为网络管理的重要组成部分。

3.4.1 IP 地址访问限制

默认情况下,IIS 会自动检查每个来访者的 IP 地址,通过 IP 地址的访问来防止或允许某些特定的计算机、域,甚至整个网络访问站点。因此,通过 IP 地址限制来在 Internet 上排除未知用户是非常有效的方法。同时,IIS 7.0 还提供了基于 Windows 域的访问限制,管理员可以禁止或允许来自指定域的用户,访问站点或目录,该功能默认是未启用的。

1. Web 站点

(1) 在“Internet 信息服务(IIS)管理器”的“Default Web Site 主页”窗口中,双击“IPv4 地址和域限制”图标,显示如图 3-64 所示的“IPv4 地址和域限制”窗口。



图 3-64 “IPv4 地址和域限制”窗口

(2) 单击“添加允许条目”链接,打开“添加允许限制规则”对话框。系统默认选中“特定IPv4 地址”单选按钮,在对应文本框中,输入想要允许访问的单个 IP 地址即可。建议选中“IPv4 地址范围”单选按钮,并输入相应的主机 IP 地址和“掩码”,如图 3-65 所示,可以同时添加多个被允许访问的主机 IP 地址。

(3) 单击“确定”按钮,新创建的限制规则即可被添加到“IPv4 地址和域限制”列表中。“添加拒绝条目”的操作步骤与之类似,此处不再赘述。

(4) 在“操作”列表中单击“编辑功能设置”链接,显示如图 3-66 所示的“编辑 IP 和域限制设置”对话框,用户还可以根据域名来限制要访问的计算机。在“未指定的客户端的访问权”下拉列表框中,设置除指定的 IP 地址外的客户端,访问该网站时所进行的操作,用户可以根据需要在下拉列表框中,选择“允许”或“拒绝”选项。若选中“启用域名限制”复选框,即可启用域名限制。需要注意的是,通过域名限制访问会要求 DNS 反向查找每一个链接,这将会严重影响服务器的性能,建议不要使用。

(5) 在“操作”列表中单击“恢复为继承的项”链接,显示如图 3-67 所示的“IPv4 地址和域限制”对话框,恢复功能以从父配置中继承设置,该操作将为当前功能删除本地配置设置(包括列表中的项目),应慎重使用。



图 3-65　“添加允许限制规则”对话框



图 3-66　“编辑 IP 和域限制设置”对话框

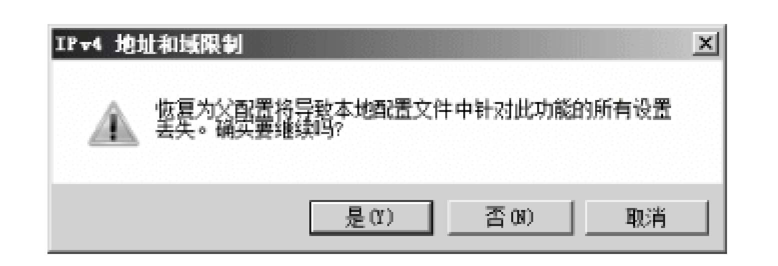


图 3-67　“IPv4 地址和域限制”对话框

(6) 在“操作”列表中单击“查看经过排序的列表”链接,显示如图 3-68 所示窗口。IIS 7.0 是按照限制规则列表中条目的顺序依次执行的。例如,当前规则列表中包括两条限制条目:拒绝 IP 地址为 192.168.1.21 的主机访问,允许整个 192.168.1.1 ~ 192.168.1.254 网段访问,即被拒绝的 IP 地址 192.168.1.21 又在被允许访问的网段内。此时,如果经过排序后拒绝在先,则将拒绝指定用户访问;如果允许在先则将允许该用户访问。

(7) 在经过排序的限制列表中,选择想要移动的限制条目,单击“上移”或“下移”链接,即可调整执行顺序。

2. FTP 站点

通过对 IP 地址的限制,同样可以只允许或拒绝某些特定范围内的计算机访问该 FTP 站点,从而可以在很大程度上避免来自外界的恶意攻击,并且将授权用户限制在某一个范围。将 IP 地址限制与用户认证访问结合在一起,将进一步提高 FTP 站点访问的安全性。特别是对于企业内部的 FTP 站点而言,采用 IP 地址限制的方式,是非常简单而有效的。

(1) 打开 FTP 站点属性对话框,切换到“目录安全性”选项卡,如图 3-69 所示,选中“拒绝访问”单选按钮,表示默认情况下所有计算机均被拒绝访问,只有将要添加的 IP 地址用户

可以访问。相反,也可以设置为默认情况下所有计算机都将被“允许访问”,然后创建需要拒绝访问的 IP 地址列表。




图 3-68 查看经过排序的列表



图 3-69 “目录安全性”选项卡

(2) 单击“添加”按钮,显示如图 3-70 所示的“授权访问”对话框,默认选中“一台计算机”单选按钮,每次只能添加一个 IP 地址。建议选中“一组计算机”单选按钮,在“网络标识”和“子网掩码”文本框中,输入相应的网络标识信息,添加一个网段内的所有 IP 地址。

(3) 单击“确定”按钮,将该所选 IP 地址或 IP 地址段添加至“下列除外”列表中,如图 3-71 所示。创建“拒绝访问”IP 地址列表的方法与之相同,此处不再赘述。

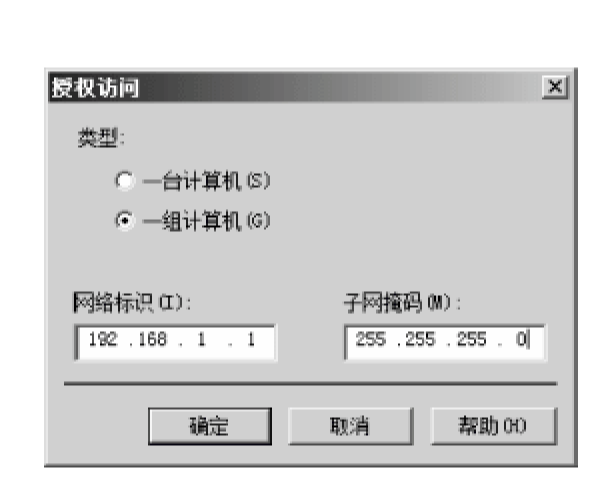


图 3-70 创建成功的授权访问 IP 地址



图 3-71 “授权访问”对话框

(4) 单击“确定”按钮,保存设置即可。

3.4.2 安全 HTTP

SSL 安全功能可以通过对传输信息进行加密,实现 Web 客户端与 Web 服务端的安全传输,避免数据被中途截获和篡改。对于安全性要求很高的、可交互性的 Web 网站,建议采用 SSL 加密方式。若欲实现 SSL 通信,Web 服务器必须拥有有效的服务器证书。

1. 创建服务器证书

要想为站点启用 SSL 安全保护,必须在服务器端创建用于 SSL 加密的证书和启用 SSL

设置。“服务器证书”包含关于服务器的信息，服务器允许客户在共享敏感信息之前，对其加以积极识别，WWW 服务器只有安装有效服务器证书后，才拥有安全通信功能。

(1) 在“Internet 信息服务(IIS)管理器”窗口中，选择希望使用 SSL 安全加密的站点，双击“服务器证书”图标，显示如图 3-72 所示的“服务器证书”窗口。安装 IIS 7.0 过程中，系统已经自动创建了一个服务器证书，管理员可以直接应用该证书，也可以导入已有证书，或者创建新的证书。这里选择“创建自签名证书”，各项操作功能含义如下。

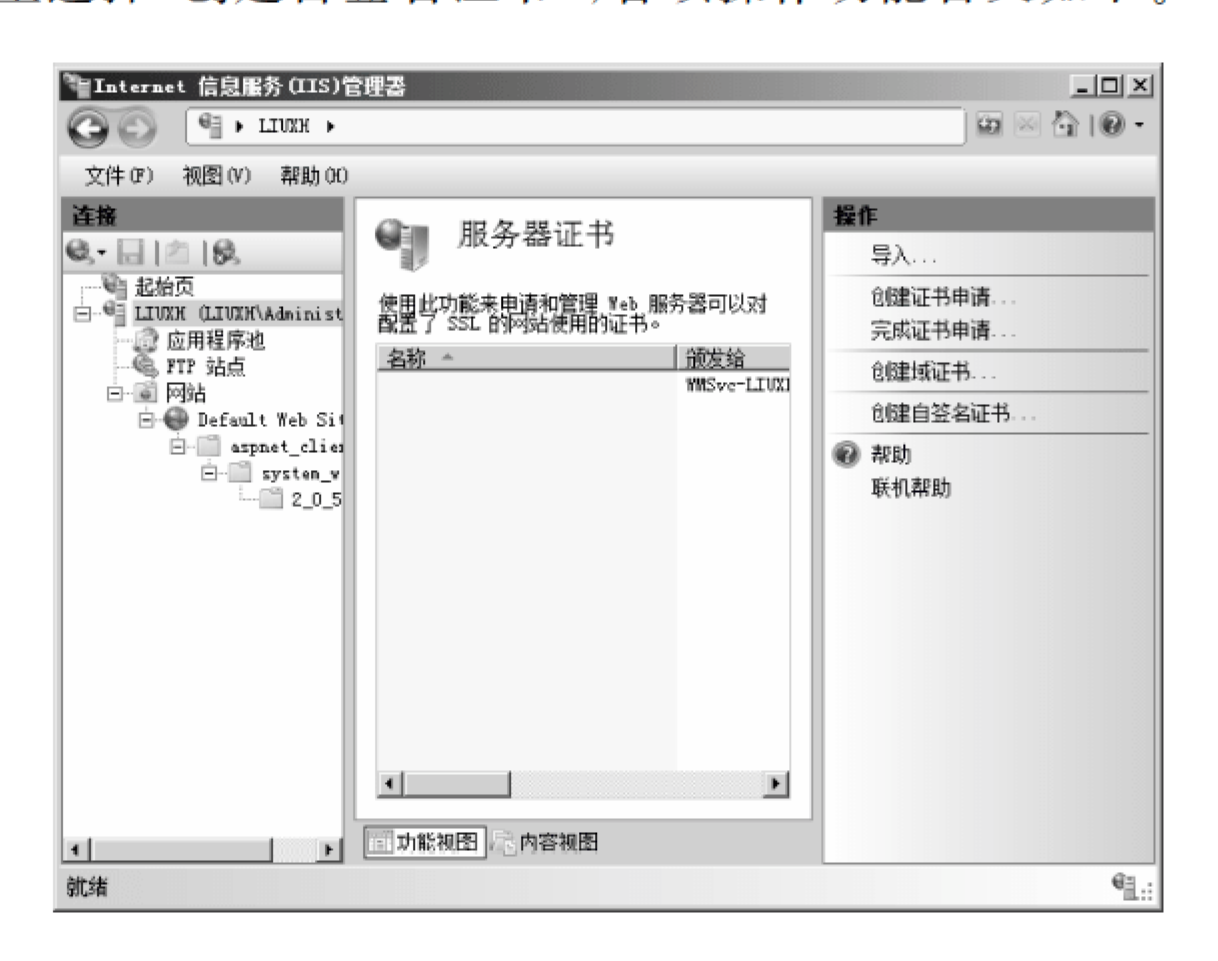


图 3-72　“服务器证书”窗口

① 导入。还原已丢失或损坏、但之前已备份的服务器证书，也可以应用来自其他用户或证书颁发机构的证书。

② 创建证书申请。如果网络存在第三方证书颁发机构(CA，证书服务器)，可以通过这种方法向证书服务器提交证书申请，通过审核后即可获得属于自己的服务器证书。

③ 完成证书申请。安装从证书颁发机构接收到的证书，并开始应用。

④ 创建域证书。向内部证书颁发机构提供有关当前服务器的信息。

⑤ 创建自签名证书。创建仅在服务器测试环境中使用并且可用于排除第三方证书故障的证书，无须向第三方服务器提交和等待批准。

⑥ 查看。查看所选证书的详细信息。

⑦ 导出。导出所选证书的备份，可以继续应用于其他目标服务器，或保存为备份，以便重新安装服务器或证书损坏后，可以快速导入。

⑧ 删除。删除选择的证书。

(2) 在右侧“操作”列表中，单击“创建自签名证书”链接，显示如图 3-73 所示的“创建自签名证书”对话框。在“为证书指定一个好记名称”文本框中，输入服务器证书的文件名。单击“确定”按钮，创建自签名证书完成，新创建的证书即可显示在列表中，选中创建成功的自签名服务器证书 safe_site，单击“查看”链接，可以查

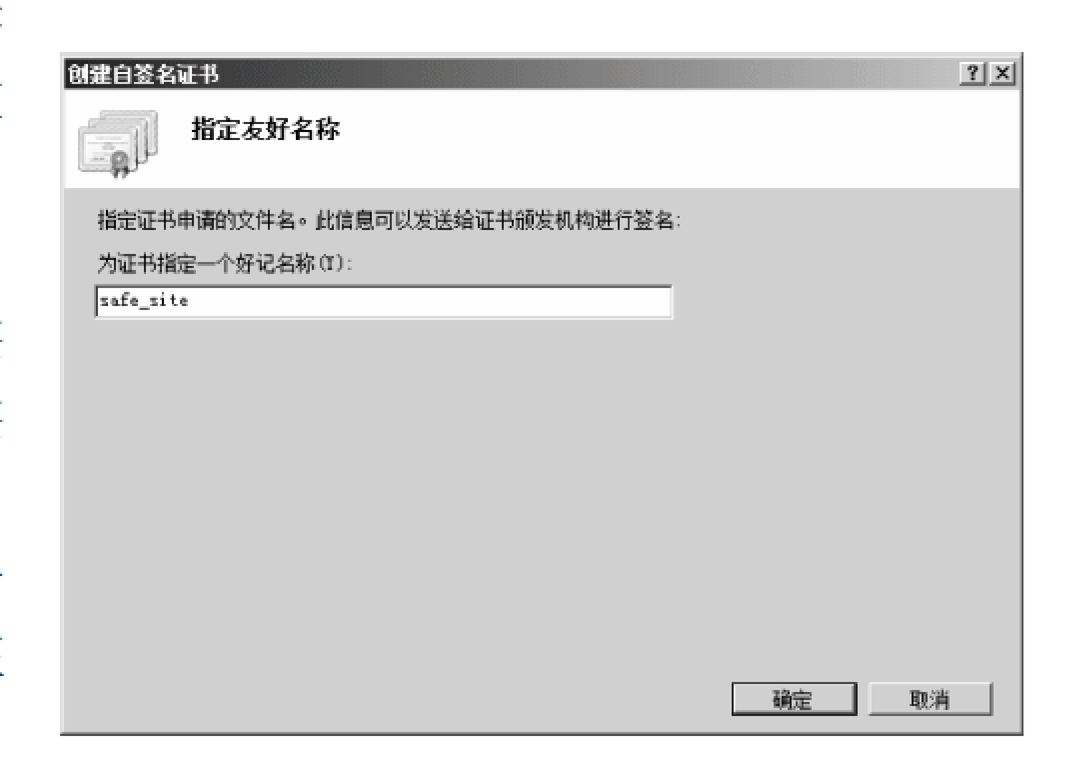


图 3-73　“创建自签名证书”对话框

看该证书的名称、颁发者、颁发给、到期日期等详细信息。

(3) 在“Internet 信息服务(IIS)管理器”窗口的“网站”列表中,右击希望应用此证书的站点(注意,必须是 https 站点),选择快捷菜单中的“编辑绑定”选项,显示如图 3-74 所示的“网站绑定”对话框。

(4) 选中 https 站点并单击“编辑”按钮,显示如图 3-75 所示的“编辑网站绑定”对话框,“IP 地址”和“端口”设置保持默认即可。在“SSL 证书”下拉列表框中,选择刚刚创建的自签名证书 safe_site。




图 3-74 “网站绑定”对话框



图 3-75 “编辑网站绑定”对话框

(5) 单击“确定”按钮,返回“网站绑定”对话框。单击“关闭”按钮保存设置并退出。

2. 启用 SSL 设置

在“Internet 信息服务(IIS)管理器”窗口中,单击需要启用 SSL 设置的站点,并在主窗口中双击“SSL 设置”图标,显示如图 3-76 所示的“SSL 设置”窗口。



图 3-76 “SSL 设置”窗口

选中“要求 SSL”复选框,以启用 40 位数据加密方法,该方法可以用来帮助确保服务器与客户端之间的传输的安全性。该选项设置既可用于 Intranet 环境,也可用于 Internet 环

境。如果选中“需要 128 位 SSL”复选框,则安全性更高,不过传输加密数据所需的带宽也将随之增加。

在“客户证书”选项区域中选中“接受”单选按钮,即可启用服务器端的 SSL 设置,接受客户端证书(若提供),在允许客户端获得内容访问权限之前验证客户端身份。系统默认选中“忽略”单选按钮,即如果提供客户端证书,则该设置不会接受,因此该设置的安全性最低。如果选中“必需”单选按钮,则在接受用户访问之前要求提供对应证书,验证客户端身份的有效性。

设置完成后,在“操作”栏中单击“应用”链接即可应用设置。

3. 客户端设置

用户访问使用 SSL 协议加密的站点或网页,与访问普通站点略有不同。首先,使用加密传输的站点使用 https://开头的 URL;其次,用户必须连接到站点指定的证书服务器,获取相关数字证书并安装。

3.4.3　知识链接:身份验证

在 IIS 7.0(Internet Information Services)中,支持以下 7 种身份验证方法,可以确认任何请求访问网站的用户的身份以及授予访问站点公共区域的权限,同时又可防止未经授权的用户访问专用文件和目录。IIS 7.0 支持的身份验证方式如下。

(1) ASP.NET 模拟身份验证。启用该身份验证方式后,ASP.NET 应用程序可以在两种环境中运行,即作为通过 IIS 身份验证的用户或作为管理员设置的任意账户。该身份验证方式需要 ASP.NET 扩展组件的支持。

(2) Forms 身份验证。使用 Forms 身份验证,可以为公共服务器上的高流量网站或应用程序提供身份验证。该身份验证模式,可以使用户在应用程序级别管理客户端注册,而无须依赖操作系统提供的身份验证机制。

(3) 基本身份验证。基本验证会“模仿”一个本地用户(即实际登录到服务器的用户),在访问 WWW 服务器时登录。因此,若欲以基本验证方式确认用户身份,用于基本验证的 Windows 用户,必须具有“本地登录”用户权限。默认情况下,主域控制器(PDC)中的用户账户,不授予“本地登录”用户的权限。使用基本身份验证方法,将导致密码以未加密形式在网络上传输。蓄意破坏系统安全的用户,可以在身份验证过程中使用协议分析程序,破译用户和密码。

(4) 摘要式身份验证。摘要式验证只能在域中使用。域控制器必须具有所用密码的纯文本复件,以便完成散列操作结果与浏览器发送散列值的比较。

(5) 匿名身份验证。这是 IIS 7.0 默认使用的身份验证方式,允许任何用户访问任何公共内容,而不用向客户端浏览器提供用户名和密码质询。如果某些内容只应当由选定用户查看,而且准备使用匿名身份验证,则必须配置相应的 NTFS 文件系统权限,防止匿名用户访问这些内容。如果希望只允许注册用户查看选定的内容,则必须为这些内容配置适当的身份验证方法,如基本身份验证或摘要式身份验证。

(6) Windows 身份验证。集成 Windows 验证是一种安全的验证形式,需要用户输入用户账户和密码。用户名和密码在通过网络发送前会经过散列处理,因此可以确保安全性。当启用 Windows 验证时,用户的浏览器通过 WWW 服务器进行密码交换。Windows 身份

验证使用 Kerberos v5 验证和 NTLM 验证。如果在 Windows 域控制器上安装了 Active Directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。

(7) 证书。可以用来建立安全套接字层(SSL)连接的数字凭据，也可以用于验证。

当不允许用户匿名访问时，还应当为 IIS 用户账户设置强密码，以实现 IIS 的访问安全。密码应该足够复杂且够长，可以通过使用数字、符号和英文字母(包括大小写)结合的方式来设置密码，长度一般在 6 位以上，并且通过经常修改密码，封锁失败的登录尝试，以及设定账户的有效期等方法对一般用户账户进行管理。

如果 IIS 服务器在域环境中运行，则还将安装一种仅适用于域环境的身份验证方式，即“Active Directory 客户证书身份验证”。允许用户使用 Active Directory 目录服务功能，将用户映射至客户证书，以便进行身份验证。将用户映射至客户证书可以自动验证用户的身份，而无须使用基本、摘要式或集成 Windows 身份验证等其他身份验证方法。

习题

1. 什么是只读域控制器，简述其在企业网络中的主要应用。
2. 什么是组作用域，不同作用域的组的功能有哪些区别？
3. 如何在不重新启动计算机的情况下，重新启动 Windows Server 2008 系统的活动目录服务？
4. 如何为 NTFS 分区上的文件和文件夹配置 NTFS 访问权限？
5. 配置 NTFS 访问权限时应遵循哪些原则？

实验：委派管理权限

实验目的：

掌握权限委派在域控制器管理中的应用。

实验内容：

将向域中添加计算机的权利委派给指定的域用户账户。

实验步骤：

(1) 以管理员账户登录域控制器。

(2) 创建用于权限委派的用户账户。

(3) 启动权限委派向导，将向域中添加计算机的权限委派到创建好的用户账户。

(4) 登录到客户端计算机，尝试使用被委派权限的用户账户将客户端计算机加入到域。

第 4 章 chapter 4

文件权限管理

文件安全是网络安全的重要课题之一，既要确保网络用户能够正常使用所需的文件，又要防止其滥用，确保文件的安全性。通常情况下，可以通过为文件设置适当的访问权限，限制用户的非法访问，达到访问控制的目的。在 Windows Server 2008 系统中，还提供了 AD RMS 文件安全保护功能，可以确保局域网内文件的安全访问。

4.1 文件权限安全规划

文件权限安全管理主要是针对安全性要求较高的文件而言的，例如商业机密、私人信函等。对于一个中型机构而言，这些信息显然是必不可少的，如何确保这些文件的访问安全已经成为网络安全管理员的一项重要工作。

4.1.1 案例情景

企业网络中有些信息是可以共享使用的，甚至可以发布到网络上，以供所有客户和用户下载使用，但是有些信息是绝对需要保密的，例如公司财务数据、产品配方、图纸、预期策划、客户资料、职工信息等。目前，最主要的信息安全保护措施就是基于文件服务器的基本安全管理，以及对普通客户端计算机的使用限制，如禁止使用 U 盘、刻录机和软盘等。

4.1.2 项目需求

现有安全防御措施虽然可以从一定程度上杜绝公司机密信息外泄，但对客户端用户的正常应用带来一些不利影响，迫切需要更好的解决方案。例如，即使员工要借助 U 盘转移一些普通文件也无法实现。

企业内部机密信息的安全防护，存在如下方面的需求。

(1) 文件在生命周期内的安全防护。这是安全防御的重中之重，大部分机密信息是有时间限制的，在此期间内，应确保文件不被破坏、窃取和恶意更改。

(2) 多人共享文件时应确保文件不被非法获取，即对机密信息的用户实施严格身份验证，确保身份的有效性，并做好详细的访问记录。

(3) 过期文件安全处理。对于一些不需要继续保密的机密文件应采取妥善的处理措施，可以永久销毁，也可以将其转为普通文件存储。

(4) 禁止非法访问。在文件保密期间，除严格限制访问用户的身份验证工作之外，还应

严格控制访问权限,例如禁止随意复制、打印或编辑机密文件等。

4.1.3 解决方案

企业网络中现有的保护措施已经可以确保机密文件的物理安全,文件访问权限的安全防护可以通过如下方案解决。

1. AD RMS

通过为文件应用 AD RMS 权限保护,可以严格限制用户账户对文件的操作权限,如只读、禁止打印等。

2. IRM

如果网络中没有部署 AD RMS 服务器,也可以使用 IRM 保护机密文件的安全,严格限制访问用户的操作权限和文件的有效期。

4.2 权限管理服务

威胁文件安全的主要因素往往来自内部用户,而普通的访问权限限定很难做到万无一失。Windows Server 2008 系统中的 AD RMS(Rights Management Services,权限管理服务)可以通过数字证书和用户身份验证技术对各种 Office 文档的访问权限加以限制,可以有效防止内部用户通过各种途径擅自泄露机密文档内容,从而确保了数据文件访问的安全性。

4.2.1 安装 AD RMS 服务器

AD RMS 服务并不是 Windows Server 2008 系统默认安装的组件,需要用户手动添加。完成必要的准备工作后,即可开始安装 AD RMS 服务器。另外,用户也可以直接安装 AD RMS 服务器,如果安装向导检测到未安装的组件,则会提示用户,此时通过选择相关选项即可一并完成准备组件的部署。

(1) 以具有管理员权限的用户账户登录到目标服务器,在"服务器管理器"窗口中,依次选择"角色"→"添加角色"选项,显示如图 4-1 所示的"选择服务器角色"对话框。选中 Active Directory Rights Management Services 复选框,提示是否添加所需的角色服务和功能,单击"添加必需的角色服务"按钮即可。

(2) 连续单击"下一步"按钮,显示"选择角色服务"对话框。如果选中"联合身份验证支持"复选框,将同时安装 AD FS 或与当前域中已有的 AD FS 关联使用,它允许用户使用当前域和其他域之间经过联合身份验证的信任关系来建立用户标识,以及提供对其他组织创建的受保护信息的访问权限。单击"下一步"按钮,显示如图 4-2 所示的"创建或加入 AD RMS 群集"对话框。系统默认选中"新建 AD RMS 群集"单选按钮。安装完成后创建的第一台 AD RMS 服务器即为根群集,后来加入的 AD RMS 服务器为叶服务器。

(3) 单击"下一步"按钮,显示如图 4-3 所示的"选择配置数据库"对话框。如果网络中安装有 SQL Server 服务器,可选中"使用其他数据库服务器"单选按钮;如果要使用 AD RMS 自带的数据库,选中"在此服务器上使用 Windows 内部数据库"单选按钮即可。

注意:选择支持 AD RMS 群集的专用数据库时应注意记录其数据库实例,其他 AD RMS 服务器加入群集时也必须指定相同的实例名称。



图 4-1 “选择服务器角色”对话框

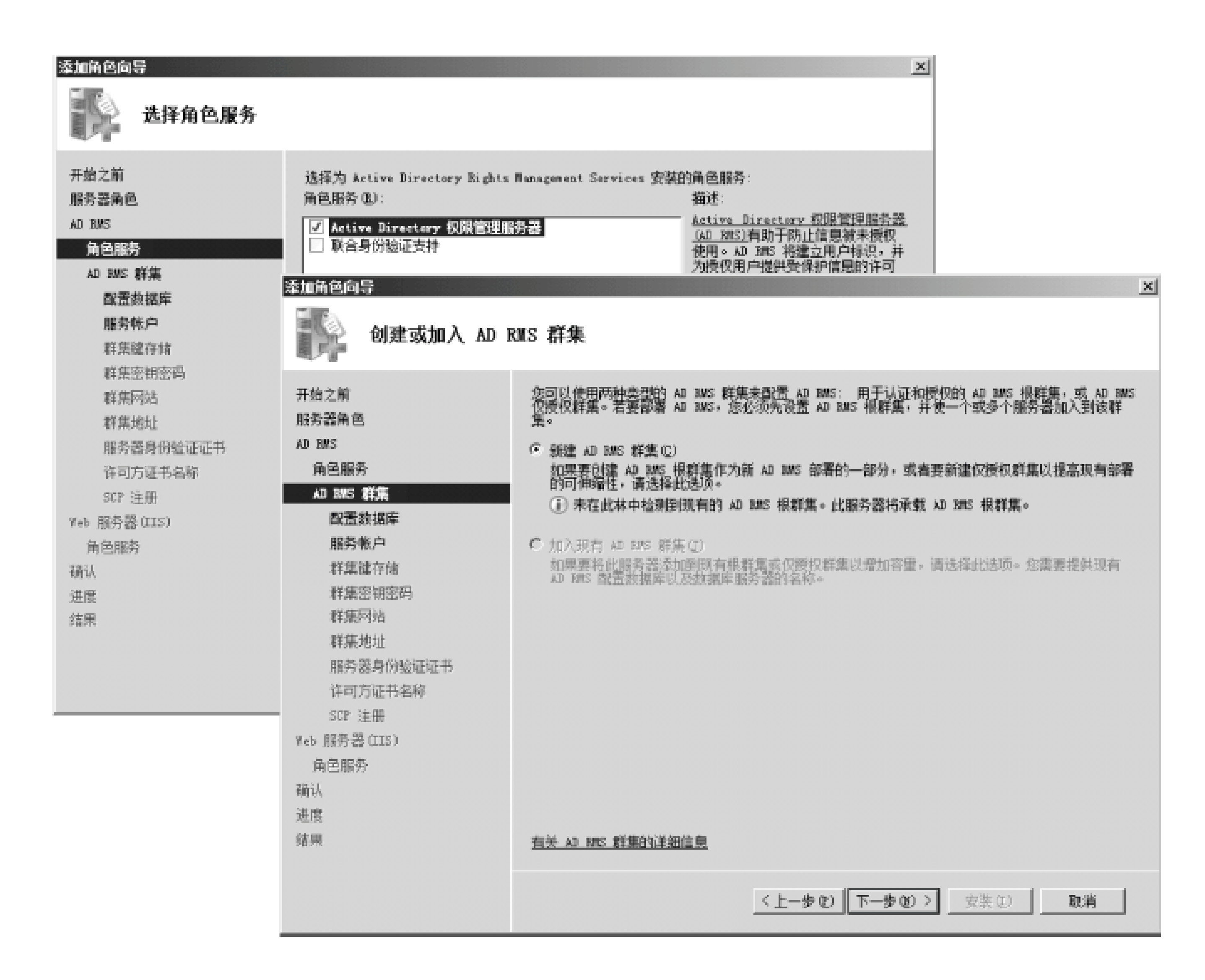


图 4-2 “创建或加入 AD RMS 群集”对话框

(4) 单击“下一步”按钮，显示如图 4-4 所示的“指定服务账户”对话框。该服务账户也就是将来要在 AD RMS 群集中使用的账户，可使用普通域成员账户，但必须区别于当前服务器登录的域用户账户。单击“指定”按钮，显示“Windows 安全”对话框，输入域用户账户。单击“确定”按钮，域控制器会对提交的用户账户和密码进行验证，如果正确无误则返回“指定服务账户”对话框。

(5) 单击“下一步”按钮，显示“配置 AD RMS 群集键存储”对话框。系统默认选中“使用 AD RMS 集中管理的密钥存储”单选按钮，即由本地服务器自动生成并存储密钥，这里选中该项，该密钥主要用于当前根服务器以及将来叶服务器的灾难恢复，必须牢记。选中“使用 CSP 密钥存储”单选按钮，则需要由专用加密服务器产生并保管该密钥，比较烦琐，但安

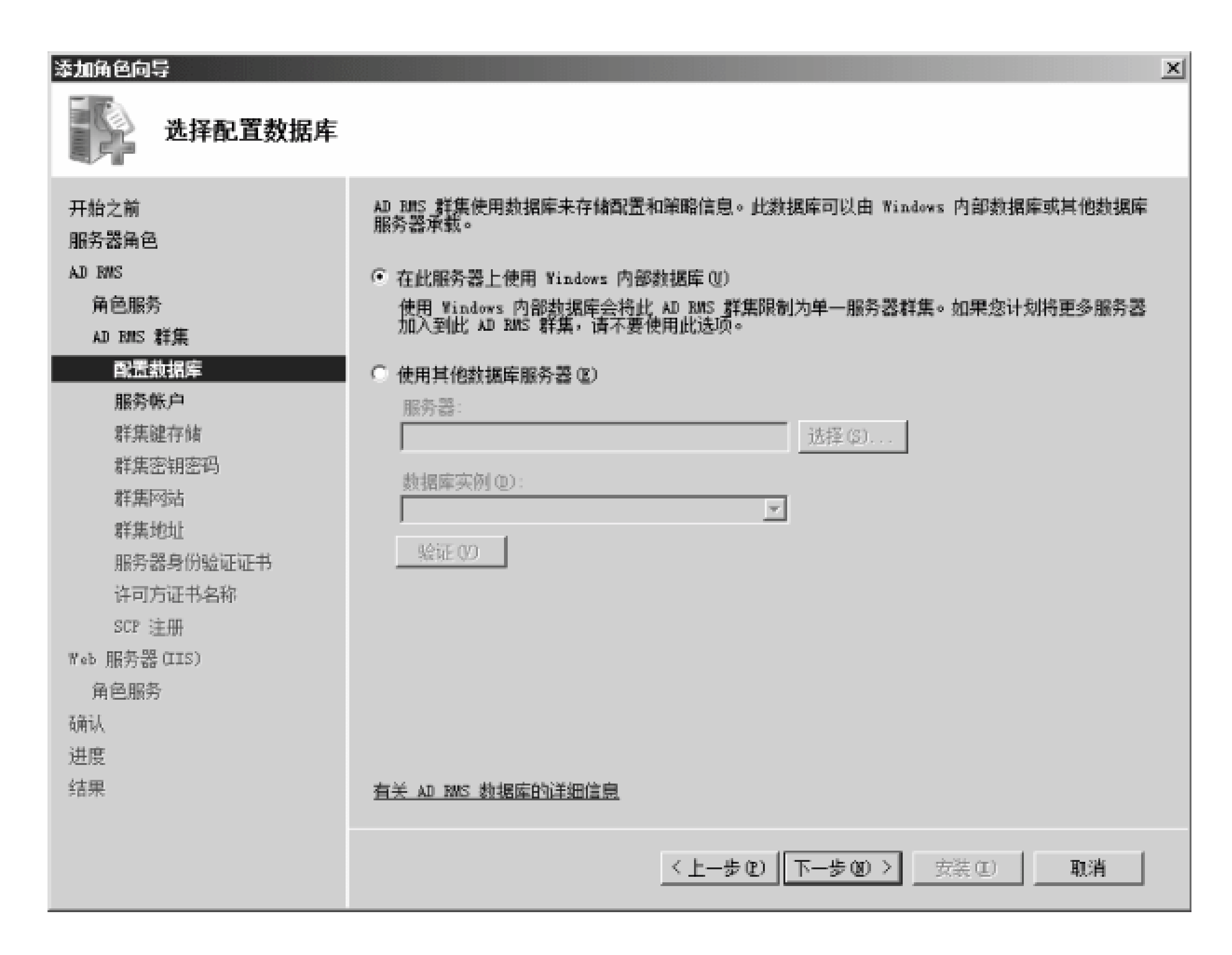


图 4-3 “选择配置数据库”对话框



图 4-4 “指定服务账户”对话框

全性也相对较高。单击“下一步”按钮，显示如图 4-5 所示的“指定 AD RMS 群集密钥密码”对话框，其他 AD RMS 服务器加入群集时也要使用此密码，必须妥善保存。

(6) 单击“下一步”按钮，显示“选择 AD RMS 群集网站”对话框，即管理 AD RMS 群集服务器时使用的站点，保持默认即可。单击“下一步”按钮，显示如图 4-6 所示的“指定群集地址”对话框。群集地址可以使 AD RMS 客户端通过网络与群集通信。选中“使用未加密的连接”单选按钮，则使用普通传输方式，输入域名，并单击“验证”按钮，确认不与其他站点冲突。

注意： 自定义端口也可以提升网络连接的安全性，不过，客户端访问时也必须使用相同的端口。

提示： 如果选中“使用 SSL 加密的连接”单选按钮，则还需要选择希望用于 SSL 加密的数字证书，可以来自网络中的 CA，也可以使用自签名证书，这里不作详细介绍。

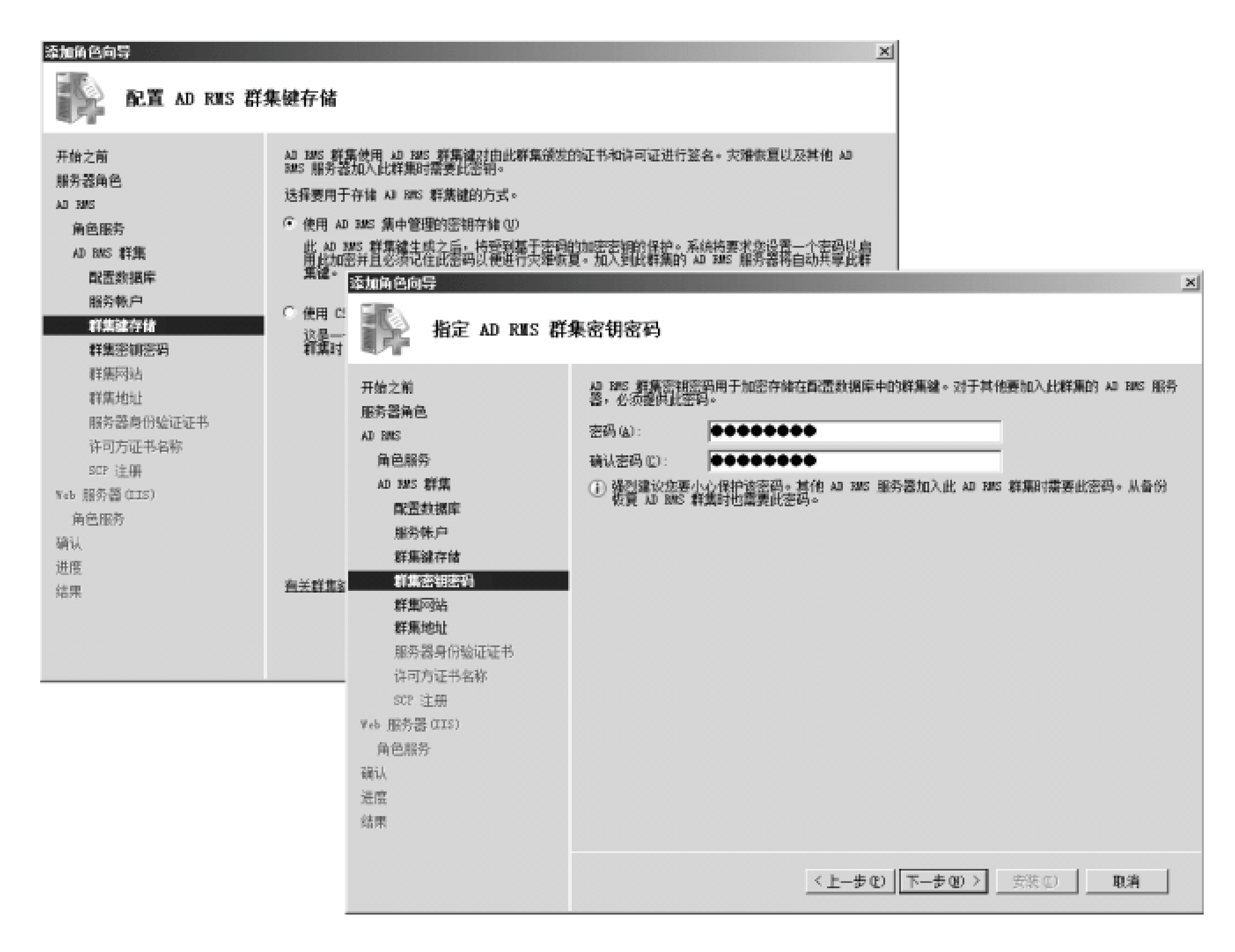


图 4-5　“指定 AD RMS 群集密钥密码”对话框



图 4-6　“指定群集地址”对话框

（7）单击“下一步”按钮，显示“命名服务器许可方证书”对话框，该对话框与上述选中的“使用 SSL 加密的连接(https://)”单选按钮是对应的，系统默认会以计算机名命名证书，保持默认即可。单击“下一步”按钮，显示如图 4-7 所示的“注册 AD RMS 服务连接点”对话框。选中“立即注册 AD RMS 服务连接点”单选按钮，在安装完成后即可使用此 AD RMS 群集。

（8）单击“下一步”按钮，将显示 IIS 的安装对话框。这里不再赘述。在“确认安装选择”对话框中，显示了要安装的组件信息。单击“安装”按钮即可开始安装。完成后显示如图 4-8 所示的“安装结果”对话框，提示安装成功。

（9）单击“关闭”按钮，退出安装向导。根据提示信息，注销当前系统并重新登录。



图 4-7 “注册 AD RMS 服务连接点”对话框



图 4-8 “安装结果”对话框

4.2.2 配置信任策略

依次选择“开始”→“管理工具”→Active Directory Rights Management Services 选项，启动 AD RMS 控制台。如果选择 SSL 加密连接的方式，则在此过程中可能会出现“安全警报”提示框，直接单击“是”按钮跳过即可。信任策略是不同 AD RMS 群集或不同域林中的 AD RMS 服务器之间建立信任关系的唯一标准，主要包括“受信任的用户域”和“受信任的发布域”。

1. 受信任的用户域

默认情况下，只有受信任的用户域才可以使用当前 AD RMS 服务器提供的权限保护服

务，不同 AD RMS 群集或不同林中的 RMS 服务器都是通过彼此的许可证书识别的。用户可以通过将其他 AD RMS 群集中的信任用户域导出，并添加至本地服务器中，来实现对其他用户提供权限管理服务。导出的信任用户域文件中会包括原 AD RMS 服务器的许可证信息，因此建立信任关系后，来自该域的用户就可以使用当前 AD RMS 服务器提供的使用许可证。

（1）在 AD RMS 控制台窗口中，依次选择“信任策略”→“受信任的用户域”选项，显示如图 4-9 所示的“受信任的用户域”窗口。在“受信任的用户域信息”列表中默认显示的是本地用户域，右击并选择快捷菜单中的“属性”选项即可查看其详细信息。



图 4-9 受信任的用户域

（2）在右侧的“操作”列表中，单击“导入受信任的用户域”链接，显示如图 4-10 所示的“导入受信任的用户域文件”对话框，在“受信任的用户域文件”文本框中输入文件的保存路径，或单击“浏览”按钮选择；在“显示名称”文本框中，输入该用户将在列表中显示的名称，用来进行标识。

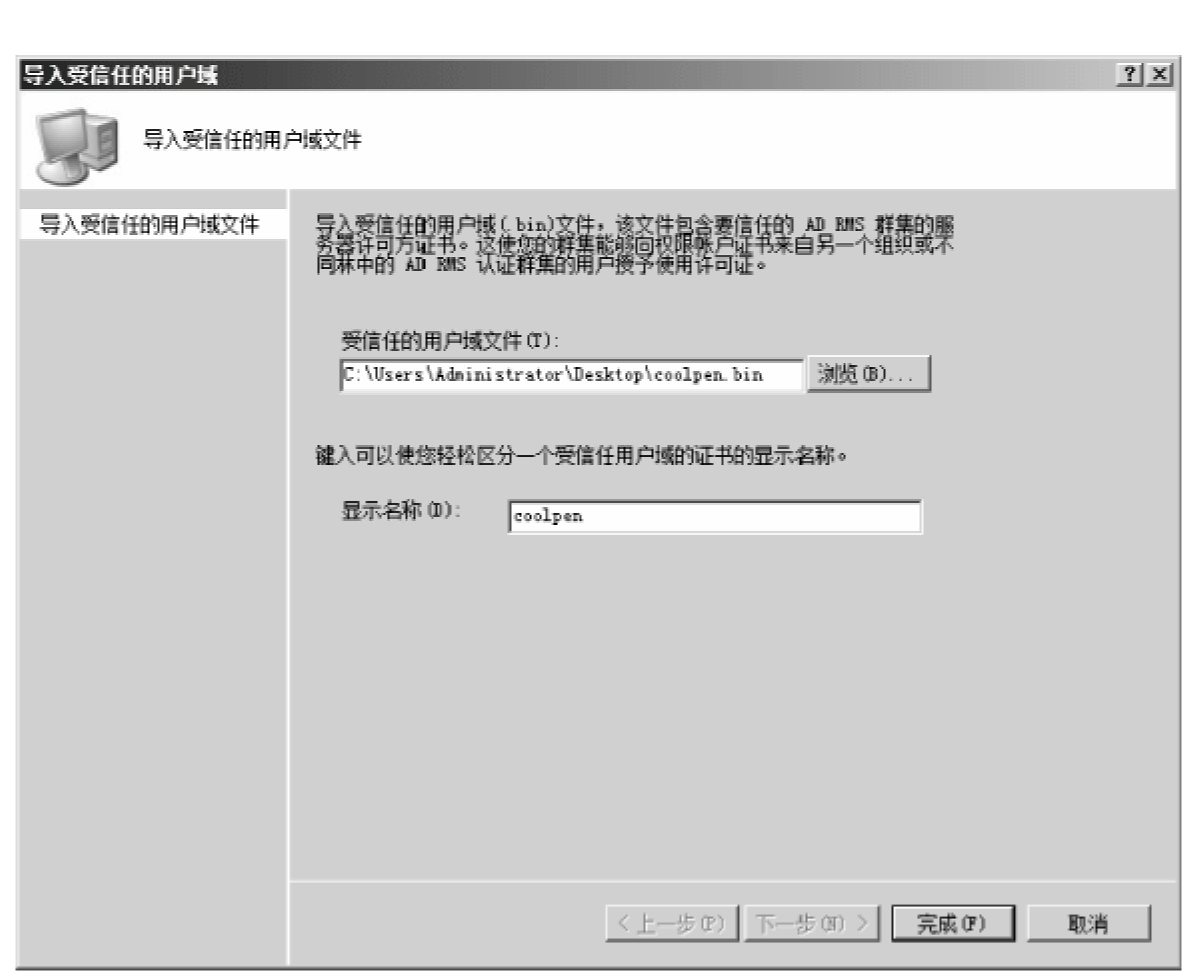


图 4-10 “导入受信任的用户域文件”对话框

（3）单击“完成”按钮，即可完成用于域的添加。重复操作，可添加多个受信任的用户域。

提示：在“受信任的用户域信息”列表中，右击域并选择快捷菜单中的“导出受信任的用户域”选项，还可以将其导出，以备本地恢复使用，也可以导入到其他 AD RMS 群集中，用于接受其他 AD RMS 服务器的权限许可证。

2. 受信任的发布域

在 AD RMS 控制台窗口中，单击“受信任的发布域”，显示如图 4-11 所示的“受信任的发布域”对话框。



图 4-11 “受信任的发布域”对话框

受信任的发布域用于定义那些 AD RMS 群集发布的许可证受到此群集的信任，与受信任的用户域恰恰相反，列表中默认存在的是本地服务器的记录。受信任的发布域文件的导出和导入与受信任的用户域文件类似，不同的是发布域文件的类型为. xml，其中包括将要信任的 AD RMS 服务器许可方证书、群集密钥和模板等信息。另外，发布域文件本身是受密码保护的，导入时必须输入原 AD RMS 服务器上使用的存储密码。

4.2.3 配置权限策略模板

1. 创建权限策略模板

机密程度不同的文档发布到客户端后设置的权限也有所不同，此时就需要为该文档应用不同级别权限的策略模板。权限策略模板是为定义用户的权限策略用的，管理员可以通过定制一些现成的策略模板让企业用户直接调用。

（1）在 AD RMS 控制台窗口中，单击“权限策略模板”显示“分布式权限策略模板”窗口。单击“操作”列表中的“创建分布式权限策略模板”链接，启动创建向导，单击“添加”按钮，显示如图 4-12 所示的“添加新的模板标识信息”对话框。在“名称”文本框中输入新建模板的名称，“描述”文本框中输入相关描述信息。单击“添加”按钮，将其添加至“模板标识”列表中。



图 4-12 “添加新的模板标识信息”对话框

提示：“语言”下拉列表框是专为使用不同语言的客户端设置的，如果客户端只支持英文显示，则可以在“添加模板标识信息”对话框中再次单击“添加”按钮，并选择“英文”语言即可。需要注意的是，要想使选择的语言生效，必须先在服务器上安装该语言。

(2) 单击“下一步”按钮，显示“添加用户权限”对话框，默认情况下“用户和权限”列表是空的，即只“授予所有者(作者)不会过期的完全控制权限”。单击“添加”按钮，显示“添加用户或组”对话框。选中“用户或组的电子邮件地址”单选按钮，即可在下面的文本框中输入用户对应电子邮件地址。如果选中“任何人”单选按钮，则对当前域中的所有用户账户有效，如图 4-13 所示。

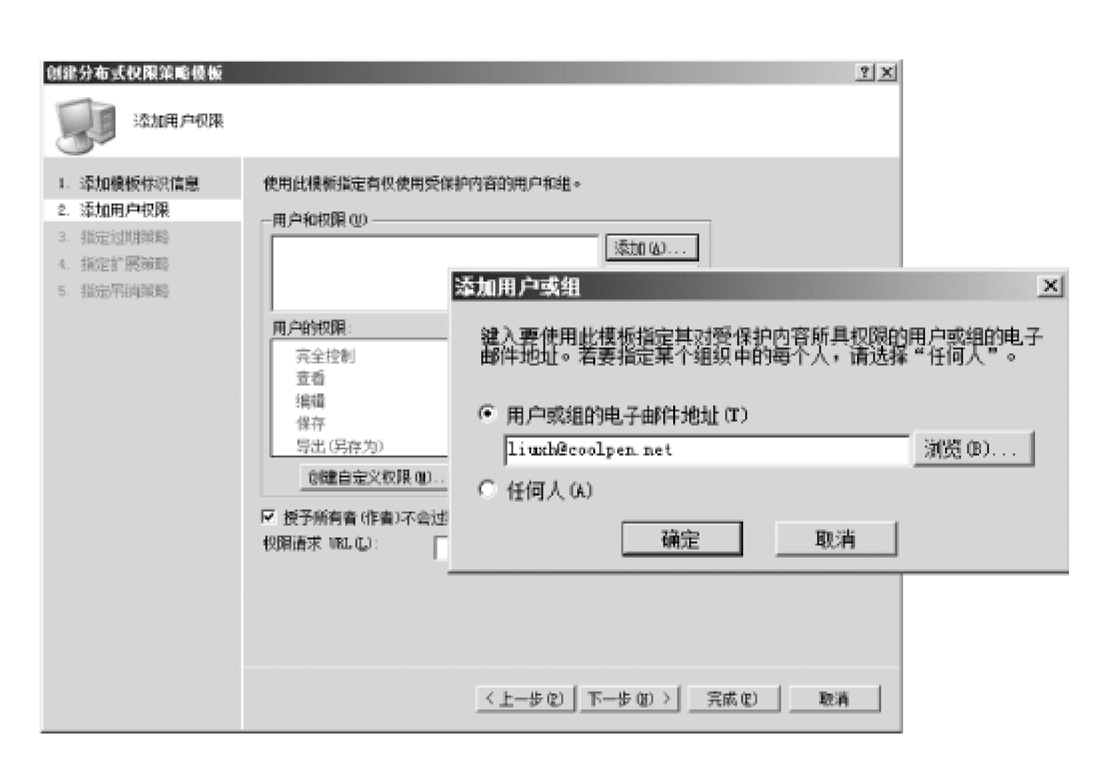


图 4-13 “添加用户权限”对话框

注意：如果要添加用户，应事先在域控制器上，打开用户属性对话框，为用户添加电子邮件地址。同样，如果要添加用户组，也要打开用户组属性，添加电子邮件地址。

(3) 单击“确定”按钮，将所选用户添加至列表中，如图 4-14 所示。重复操作，可添加多个用户或组的电子邮件地址。然后，在“用户和权限”列表中，选择赋予用户的权限，例如，要求做到“禁止复制”，则只选中“查看权限”复选框即可。

“权限请求 URL”是当模板赋予用户的权限无法完成相应工作，或在模板权限规定的时间和日期内没有完成工作时，用户可以通过此 URL 继续向管理员发出权限请求，以再次获得权限或附加权限。

注意：权限列表中给出的所有权限都是允许的，即只要选择某项，就表示要赋予用户具有相应的权限。

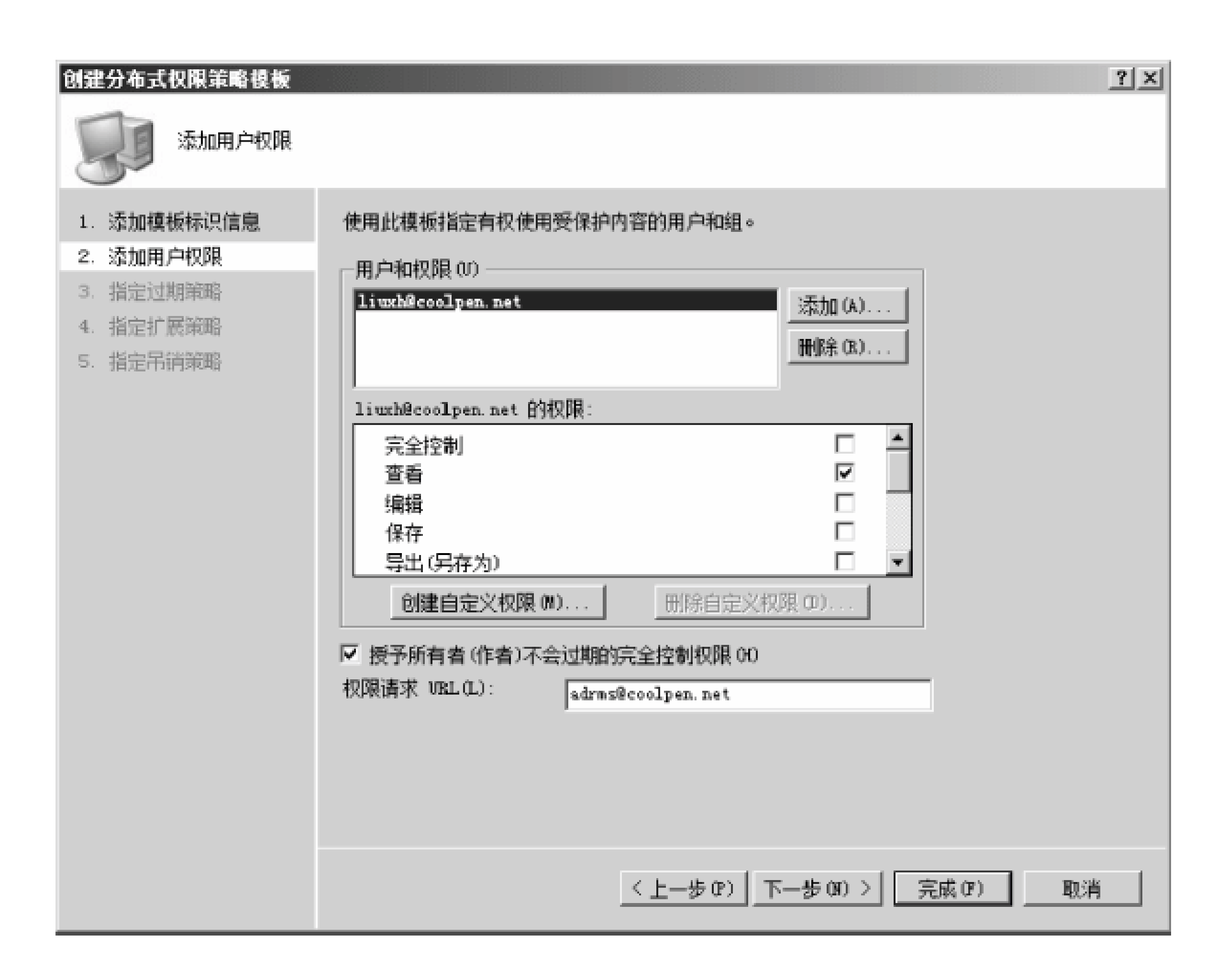


图 4-14　指定用户权限

(4) 单击“下一步”按钮，显示如图 4-15 所示的“指定过期策略”对话框。在“内容有效期限”选项区域中，可以定义当前模板中的权限信息何时过期或有效期限等，默认为“永不过期”。内容过期后，如果仍需要使用该策略信息，则必须重新发布一次。

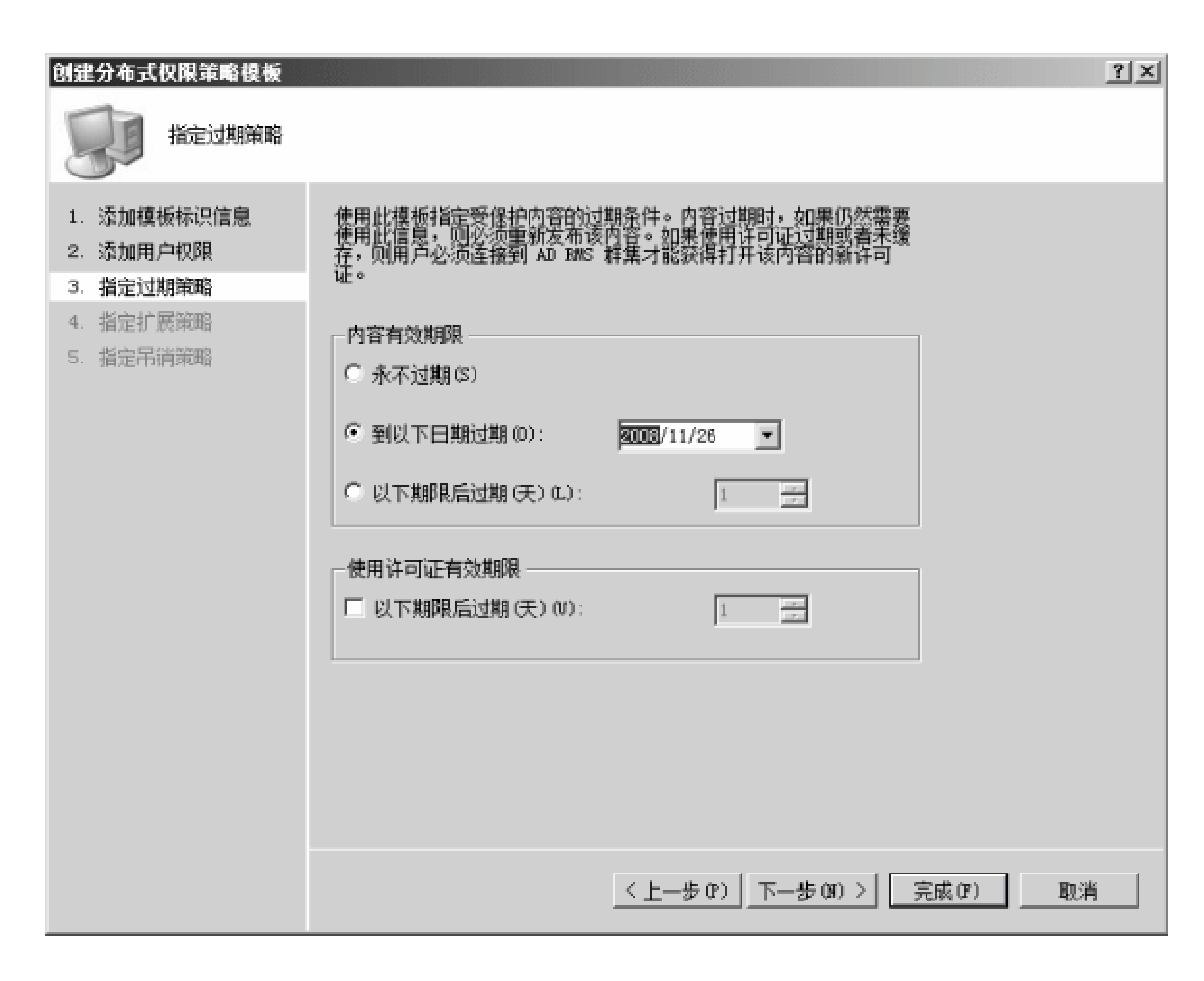


图 4-15　“指定过期策略”对话框

(5) 单击“下一步”按钮，显示“指定扩展策略”对话框，保留默认设置即可。单击“下一步”按钮，显示如图 4-16 所示的“指定吊销策略”对话框。吊销是 AD RMS 的一项重要功能，实施吊销之前必须先手动创建一个吊销列表，并为每个吊销列表生成一个公钥/私钥对，然后使用私钥签署吊销列表；另外，还必须为吊销列表指定一个用户可以访问的 URL 地址或 UNC 路径。通常情况下，不需要 AD RMS 服务器吊销，即不选中该复选框。

(6) 单击“完成”按钮，退出创建向导，返回“权限策略模板”窗口，如图 4-17 所示。新创建的模板已经出现在列表中，此时虽然已经创建成功，但并不能立即应用。

(7) 选择新创建的策略模板，右击并选择快捷菜单中的“存档此分布式权限策略模板”



图 4-16 “指定吊销策略”对话框



图 4-17 权限策略模板创建成功

选项，将其本地存档，显示“存档权限策略模板”对话框。提示一旦保存后，将不能再分发或导出该模板。单击“是”按钮保存即可。至此，新创建的权限策略模板才可以保存到本地模板库中备用。

返回“分布式权限策略模板”窗口，单击“管理存档的权限策略模板”链接，所有已存档的策略模板即可显示在“分布式权限策略模板”列表框中，管理员可以继续修改和查看其各项属性信息。图 4-18 所示是新建策略模板的权限摘要。

2. 分发权限策略模板

客户端必须将服务器上创建的权限策略模板保存到本地计算机才可以使用，可以通过文件共享、网络传输、移动存储介质等方式获得。默认情况下，权限策略模板的保存位置为“未设置”。为了便于保存和用户使用，应在群集中指定一个公共文件夹，用于保存所有的策

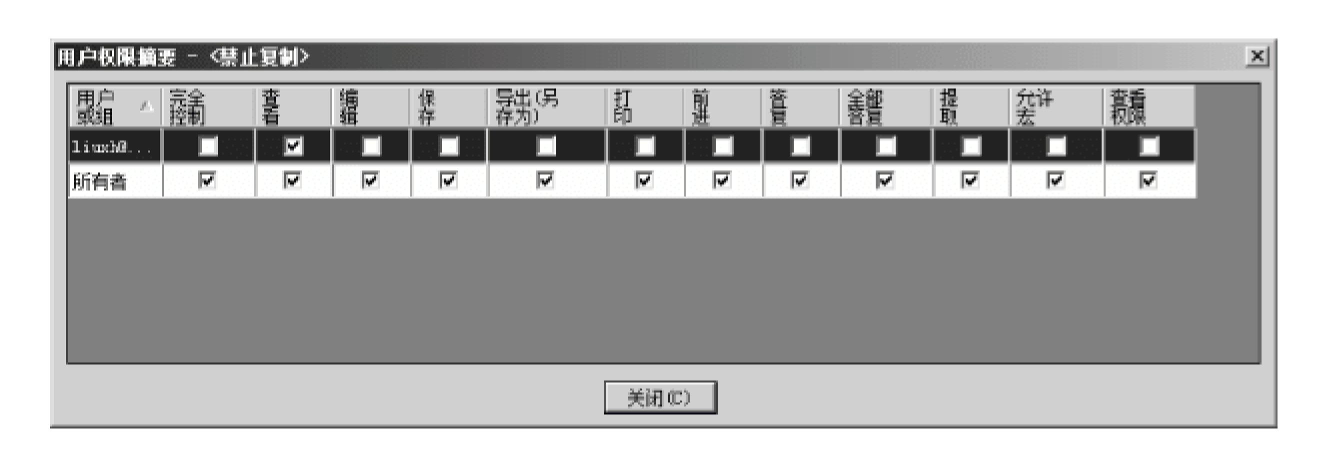


图 4-18　用户权限摘要

略模板。

（1）在“权限策略模板”窗口中，单击“操作”列表中的“管理分布式权限策略模板”链接，在“分布式权限策略模板”窗口下方单击“更改分布式权限策略模板文件位置”链接，打开如图 4-19 所示的“权限策略模板”对话框。

（2）选中“启用导出”复选框，在“指定模板文件位置(UNC)”文本框中输入已经设置好的共享文件夹路径，如图 4-20 所示。注意，这里必须使用 UNC 格式，并且确定已经为指定用户账户赋予了写入权限。

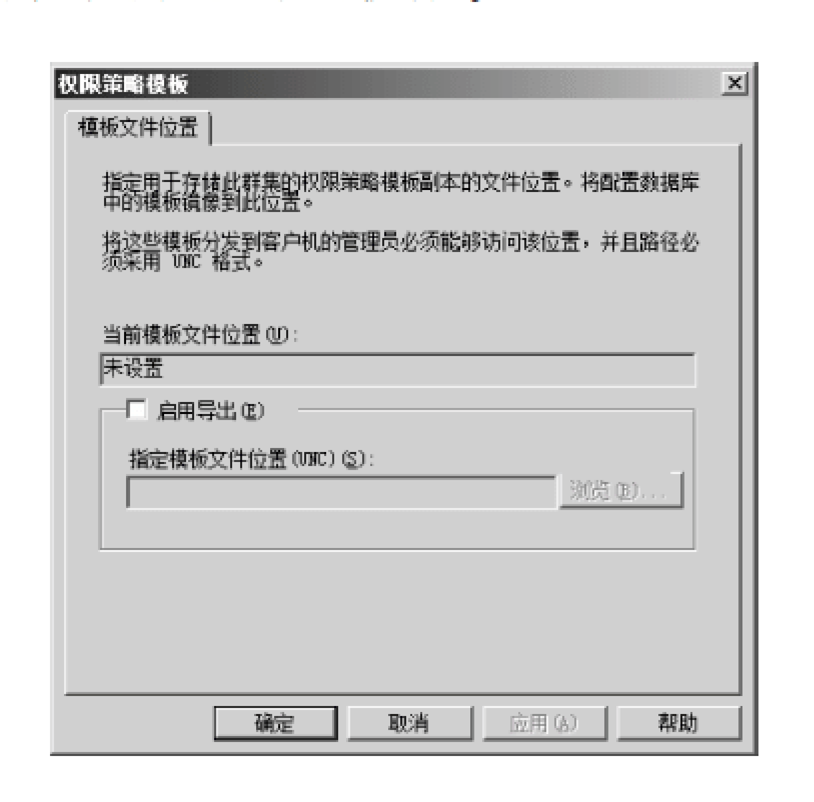


图 4-19　“权限策略模板”对话框

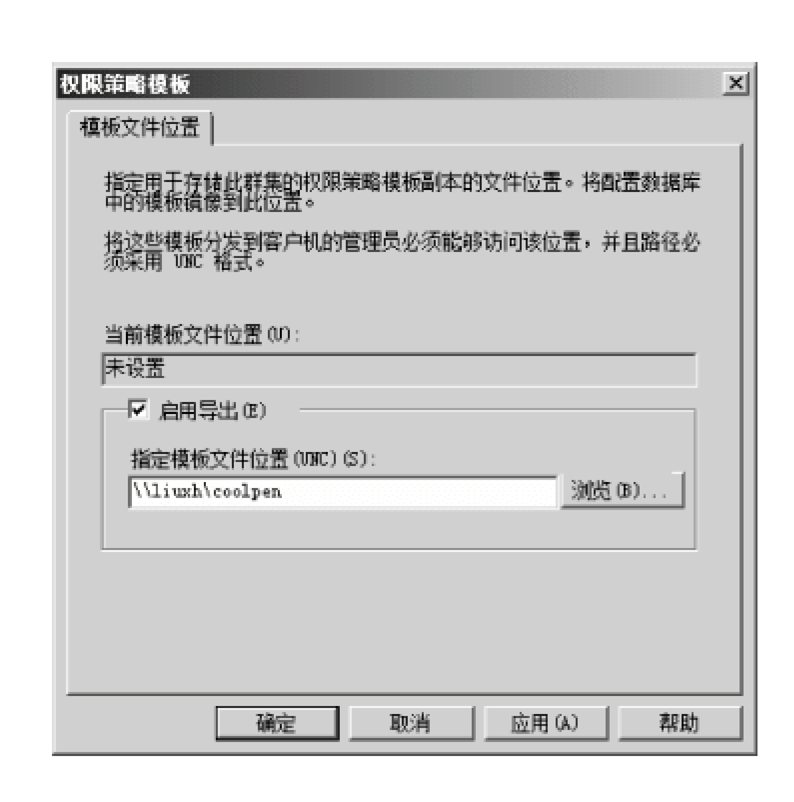


图 4-20　设置共享文件夹路径

（3）设置完成后单击“确定”按钮。然后，单击“管理存档的权限策略模板”链接，选择想要分发的模板，右击并选择快捷菜单中的“分发此权限策略模板”选项，显示“分发权限策略模板”对话框。提示分发之后，用户便可以使用此模板发布新内容。单击“是”按钮确认即可。

提示：如果模板是从另一台 RMS 服务器迁移到此 RMS 服务器，在使用该模板之前，必须由此服务器签署，然后重新分发到客户端。

4.2.4　AD RMS 客户端部署及应用

AD RMS 客户端安装过程非常简单，此处不作详细介绍。需要注意的是，更换登录的域用户账户后，应重新运行客户端安装向导，并选中“修复带 Service Pack 2 的 Windows Rights Management 客户端”单选按钮。客户端需要将服务器上创建并保存的权限策略模板复制到客户端计算机上才可以使用，另外还需要在注册表中做相应修改。

（1）通过网络共享或移动存储设备，将 AD RMS 服务器上存储的权限策略模板，复制

到本地计算机上。打开“注册表编辑器”窗口，并依次展开如下分支：

HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\DRM

在右侧窗口空白处右击，依次选择“新建”→“字符串值”选项，新建一个字符串值项目。将新创建的字符串值命名为 AdminTemplatePath，然后双击该对象或右击再选择“修改”选项打开如图 4-21 所示的“编辑字符串”对话框，指定该对象的数值数据为本地计算机上保存要应用的权限策略模板的路径。这里，将要保存在 E 盘根目录下，因此，输入 e:\即可。

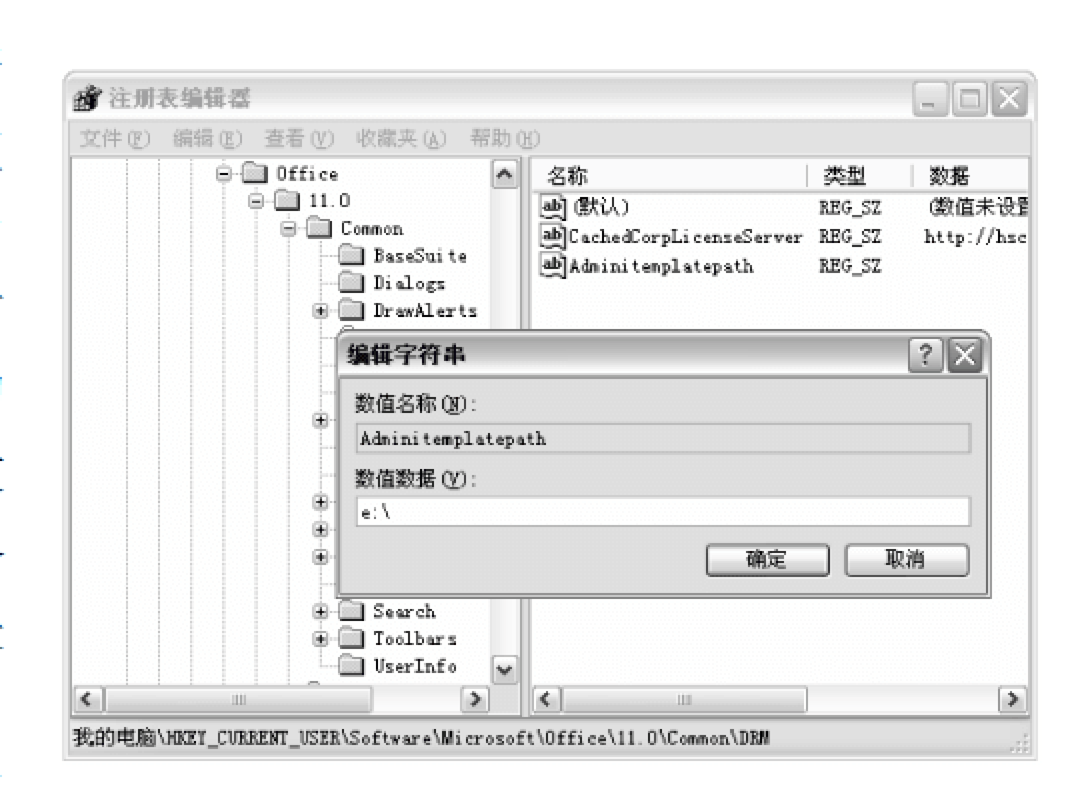


图 4-21 “编辑字符串”对话框

(2) 单击“确定”按钮，保存设置并关闭“注册表编辑器”窗口。打开欲应用此策略模板的受保护文档，打开“文件”菜单中的“权限”选项，此时，会发现级联菜单中多出了一个可选项，即“禁止拷贝”，如图 4-22 所示。

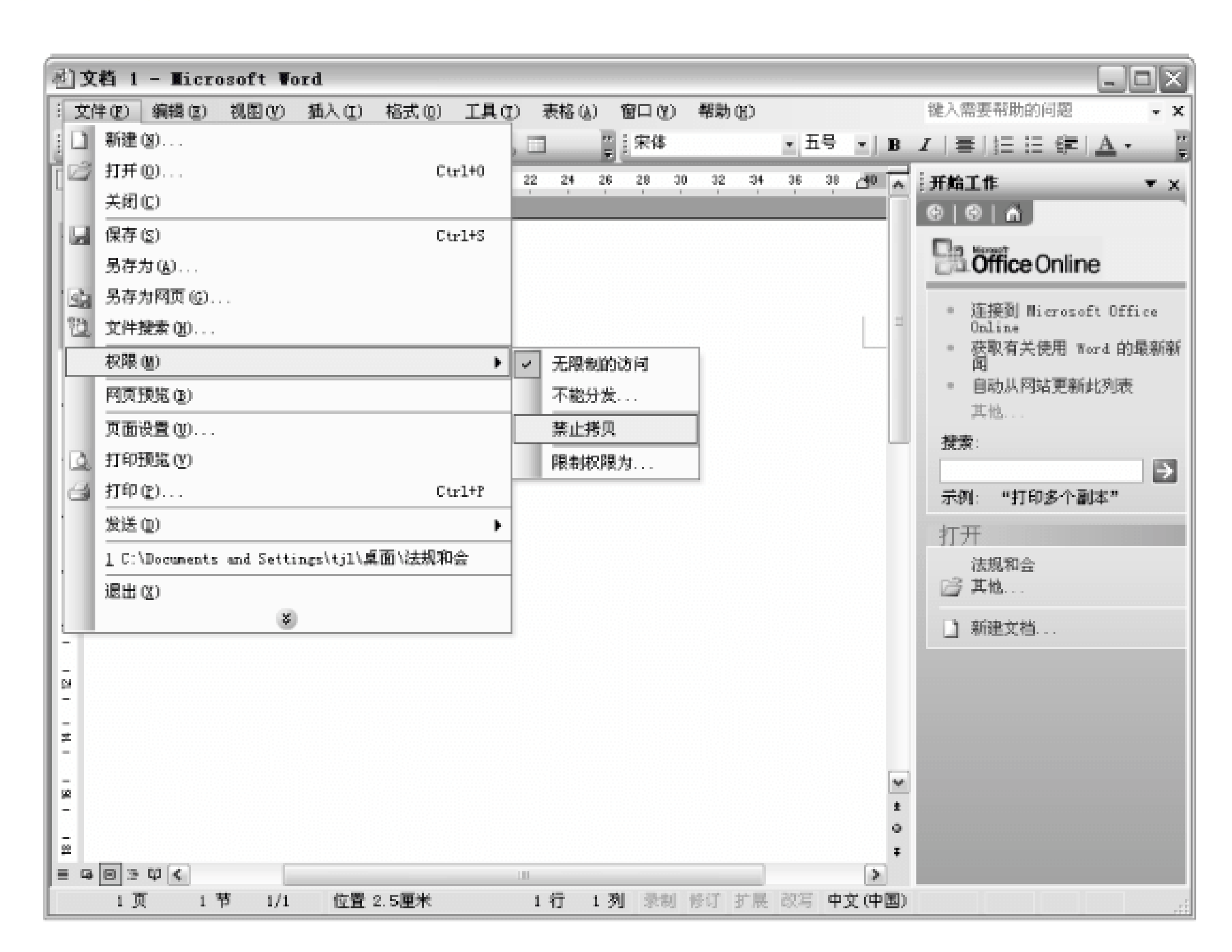


图 4-22 添加成功

(3) 选定相应策略模板后，共享工作区中会显示“受限权限”等信息。授权人信息默认是本地登录账户，当然，管理员也可以在建立到服务器的连接时指定为其他用户，或直接单击“更改用户”链接随时更改。本例是 lhn@coolpen.net(所用模板针对的用户为 tjl@coolpen.net)。单击共享工作区中的“更改权限”链接，可以查看当前用户账户对该文档拥有的控制权限，显示如图 4-23 所示对话框。由于目前登录用户是该文档的创建者，在 RMS 配置该权限策略模板时，为文档作者赋予了完全控制的权限，即所有权限的状态都是“是”。

部署 Windows Vista 系统的 AD RMS 客户端更加容易。由于默认情况下，系统已经集成 RMS 客户端功能，因此只须指定权限策略模板的路径。打开欲应用此策略模板的受保护文档(以 Office Word 2007 为例)，单击 Office 按钮，并依次选择“准备”→“限制权限”选项，



图 4-23　当前用户权限

此时，会发现级联菜单中多出了一个可选项，即“禁止复制”，如图 4-24 所示。



图 4-24　成功添加策略模板

4.2.5　受限客户端应用被保护文档

AD RMS 策略模板主要是为了限制某些客户端针对文档享有的权限，因此当这些受限客户端应用被保护文档时，必须连接到 AD RMS 服务器进行凭据验证，并下载相应权限许可证才可以打开。这里，仍以上述应用为例进行介绍。



图 4-25　受限用户打开被保护文档

(1) 当用户 lhn@coolpen.net 创建好的文档，应用了限制用户 tjl@coolpen.net 复制和更改的权限。那么，当用户 tjl@coolpen.net 拿到文档并查看时，会显示如图 4-25 所示的

提示框。

（2）单击“确定”按钮，客户端开始向 AD RMS 服务器提交身份验证，并获得相应的权限，最终打开文档，显示如图 4-26 所示的窗口。不过此时，文档是“只读”状态，并且不允许用户执行“复制”命令，或按 Print Screen 键抓取屏幕，这是因为当前被保护文档应用的权限策略模板已经屏蔽了 Windows 的这些功能，关闭受保护文档则一切恢复正常，用户使用时应注意。

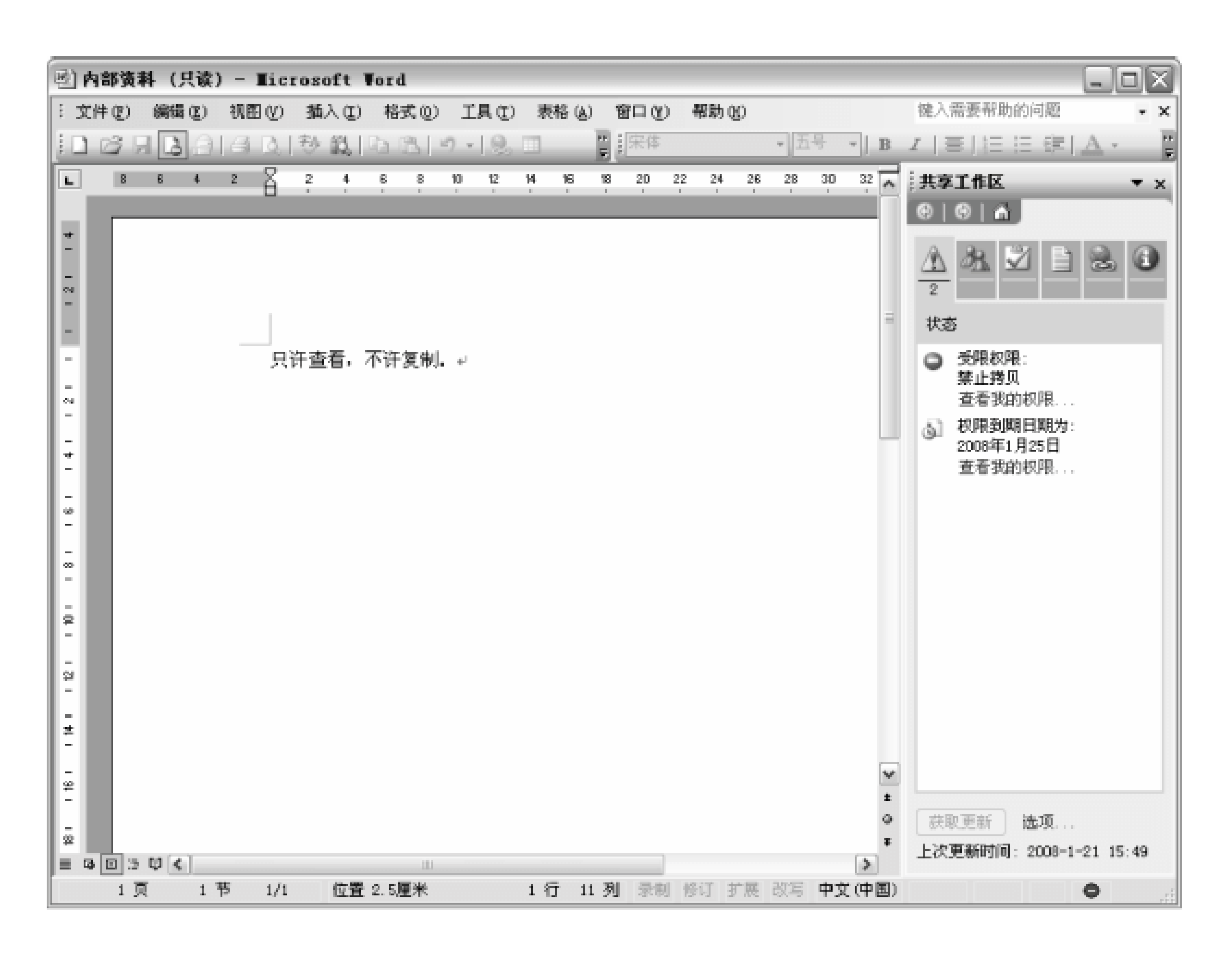


图 4-26　文档处于“只读”状态

（3）单击“查看我的权限”链接，打开如图 4-27 所示的“我的权限”对话框，其中只有“查看”一项处于“是”状态，其他均为“否”。如果当前用户权限无法完成操作，可以单击“更改用户”按钮，使用其他被赋予更高操作权限的用户账户登录。

单击“请求附加权限”链接，向 AD RMS 服务器申请相关权限，打开如图 4-28 所示的窗口。“收件人”文本框中就是 AD RMS 服务器上设定的接收申请的电子邮件地址，保持默认即可。根据自己的实际需要，说明想要请求的权限即可。

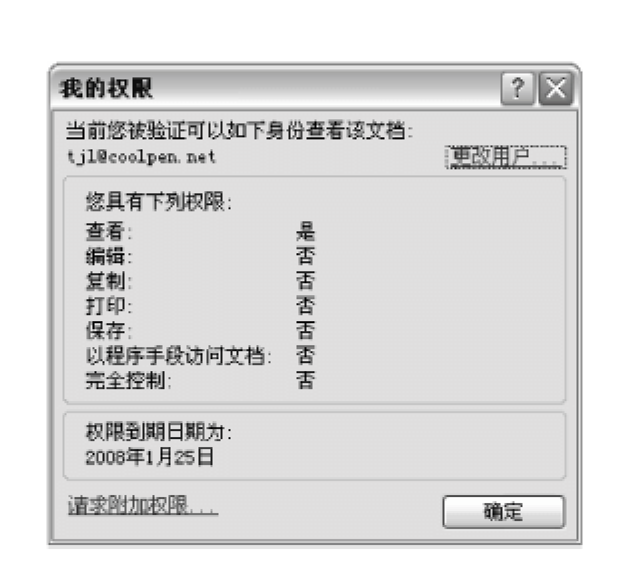


图 4-27　“我的权限”对话框

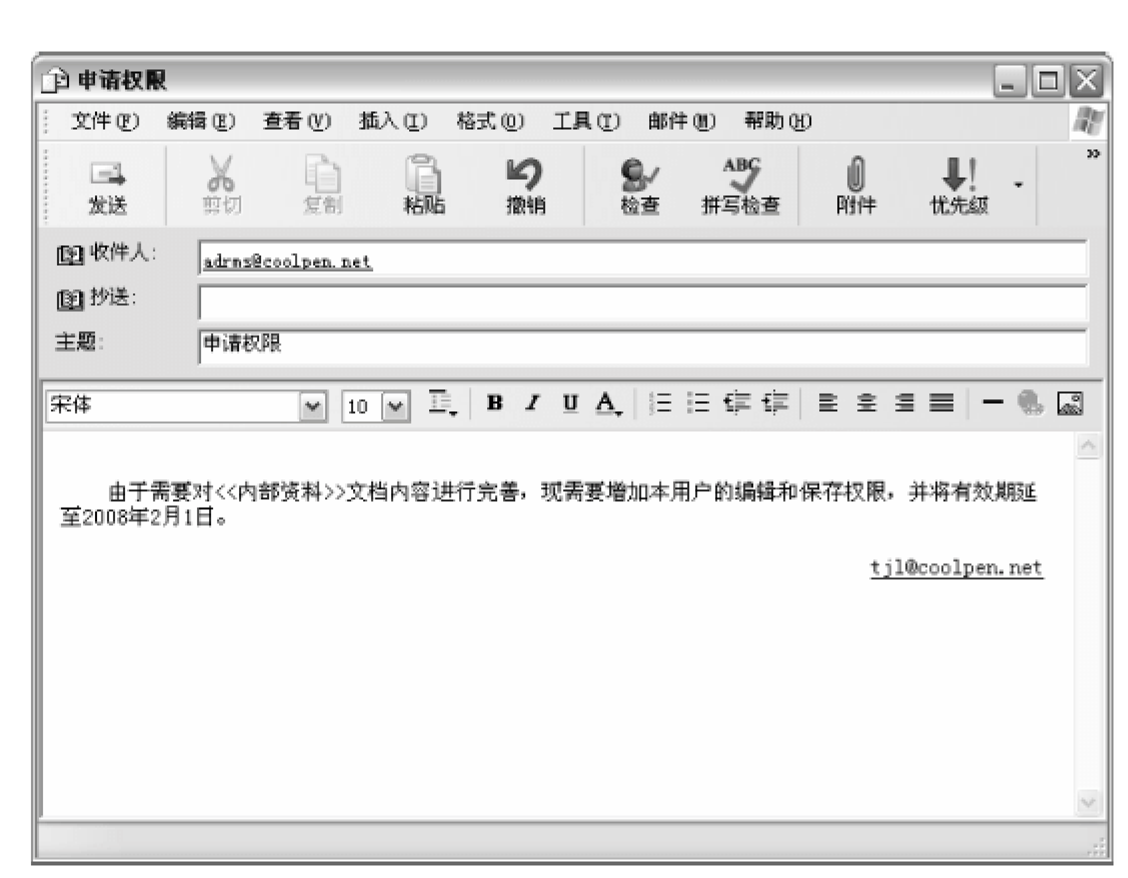


图 4-28　申请附加权限

提示：需要应用此功能时，必须先在网络中配置 Exchange 或其他邮件服务器。虽然在 AD RMS 系统中用到 E-mail 地址的地方非常多，但是多数情况下是作为一种用户标识，并非真正地用来传递信息，所以网络中邮件服务器也就可有可无。如果确实需要传递信息，则必须搭建邮件服务器。

4.2.6 知识链接：AD RMS

1. AD RMS 服务器

相对于先前的 RMS 而言，AD RMS 不再是一个独立服务插件，已经成为 Windows 的一项内建功能，并且包含了某些升级功能，可以直接在管理服务器窗口中启动安装向导即可轻松安装。为了确保安装过程可以顺利进行，开始之前应做好如下准备工作。

(1) 将计算机加入到域，或者提升为域的额外域控制器，或者子域。

(2) 使用具有域用户账户登录，但不能使用 Administrator 账户登录。

(3) 安装 IIS 服务和 ASP.NET 组件。

(4) 安装 MSMQ(消息队列)服务。

(5) 选择数据库。如果要使用独立数据库，需安装 SQL Server。否则，可使用 AD RMS 的自带数据库。

(6) 安装之前，确认 http://uddi.microsoft.com 和 https://uddi.microsoft.com 在 Internet Explorer 中被添加至"受信任的站点"或"本地 Internet"。

2. AD RMS 客户端

AD RMS 服务安装并配置完成以后，即可将需要接受 AD RMS 管理的客户端加入域，并部署 AD RMS 客户端。在 Windows Vista 系统中，RMS 客户端的名称已更改为 Active Directory 权限管理服务(AD RMS)客户端，并且已集成到操作系统中，因此不需要独立的安装。在早于 Windows Vista 的 Windows 操作系统版本中，RMS 客户端组件仍需要独立下载和安装。目前最新版本为 SP2 简体中文版下载地址为：

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=02da5107-2919-414b-a5a3-3102c7447838

提示：管理员还可以通过组策略、SMS、SCCM 等方式来向客户端统一分发客户端安装程序。如果客户端数量较少，则可以通过手动安装的方式实现。

4.3 信息权限管理

信息权限管理(Information Rights Management，IRM)是 Windows 权限管理服务(RMS)在 Office 应用程序和 Internet Explorer 中的扩展(通过一个免费的加载项)，可以有效地保护机密文件的内容，即使未被授权的用户得到文档，也无法打开文件。IRM 的授权是通过 Microsoft .NET Passport 来实现的，需要 Internet 支持。只要具备有效的 Hotmail 或 MSN 邮箱即可获得一个 Passport 账户。IRM 可以保护 Word、Excel、PowerPoint 等 Office 文档，只有 Microsoft Office 2003/2007 用户才可以使用 IRM 保护文档安全。

4.3.1　创建被保护的安全文档

IRM的应用与RMS客户端类似，只需为需要保密的文档设置权限保护即可。以Windows Vista系统中Microsoft Office Word 2007为例，操作步骤如下。

(1) 打开需要添加权限保护的文档，单击Office按钮，依次选择“准备”→“限制权限”→“限制访问”选项，显示“服务注册”对话框。选中“是，我希望注册使用Microsoft的这一免费试用服务”单选按钮。单击“下一步”按钮，显示如图4-29所示的“欢迎使用Windows RM账户证书向导”对话框，选中“是，我有.NET Passport”单选按钮。如果没有.NET Passport账户，则可以选中“否，我没有.NET Passport，我要立即注册.NET Passport”单选按钮注册账户。



图4-29　“欢迎使用Windows RM账户证书向导”对话框

(2) 单击“下一步”按钮，显示如图4-30所示的“登录到.NET Passport”对话框，在“电子邮件地址”和“密码”文本框中，输入有效的Hotmail或MSN账户信息。选中“自动登录”复选框，则再次使用该.NET Passport账户创建安全文档时，不必输入用户信息。



图4-30　“登录到.NET Passport”对话框

(3) 单击“登录”按钮，显示“选择证书类型”对话框，选中“标准”单选按钮。单击“下一步”按钮，开始登录微软Windows RM证书服务器，显示如图4-31所示的“正在完成Windows RM账户证书向导”对话框，提示已成功下载RM账户证书。

(4) 单击“完成”按钮，显示如图4-32所示的“权限”对话框，选中“限制对此文档的权限”



图 4-31 “正在完成 Windows RM 账户证书向导”对话框

复选框，在“读取”和“更改”文本框中，输入想要授予相应权限的.NET Passport 账户即可，多个账户之间需要使用分号(;)分隔。如果曾经保存过通讯簿，则可以单击“读取”和“更改”按钮，从通讯簿中选择用户账户。

单击“其他选项”按钮，显示如图 4-33 所示的“权限”对话框，这里包括修改用户访问级别、文档到期日期、请求权限地址等选项。选中“此文档的到期日期为”复选框，可以设置被保护文档的到期日期，过期之后，除文档创建者之外的任何用户，都无法使用该文档。默认情况下，已经选中“用户可以从此请求附加权限”复选框，并输入文档创建者的.NET Passport 账户，即未被授权用户可以通过发送请求，得到所需的访问权限。

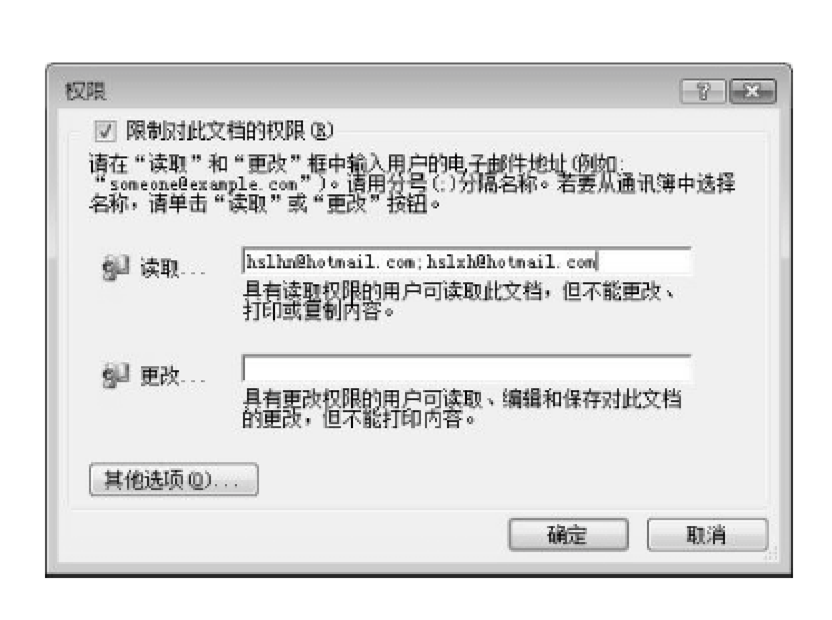


图 4-32 “权限”对话框(1)



图 4-33 “权限”对话框(2)

(5) 单击“确定”按钮，完成权限设置，如图 4-34 所示。此时，文档上方工具栏中，将显示此文档已设置限制访问，只有指定用户才可以访问此内容。单击“更改权限”按钮，可以立

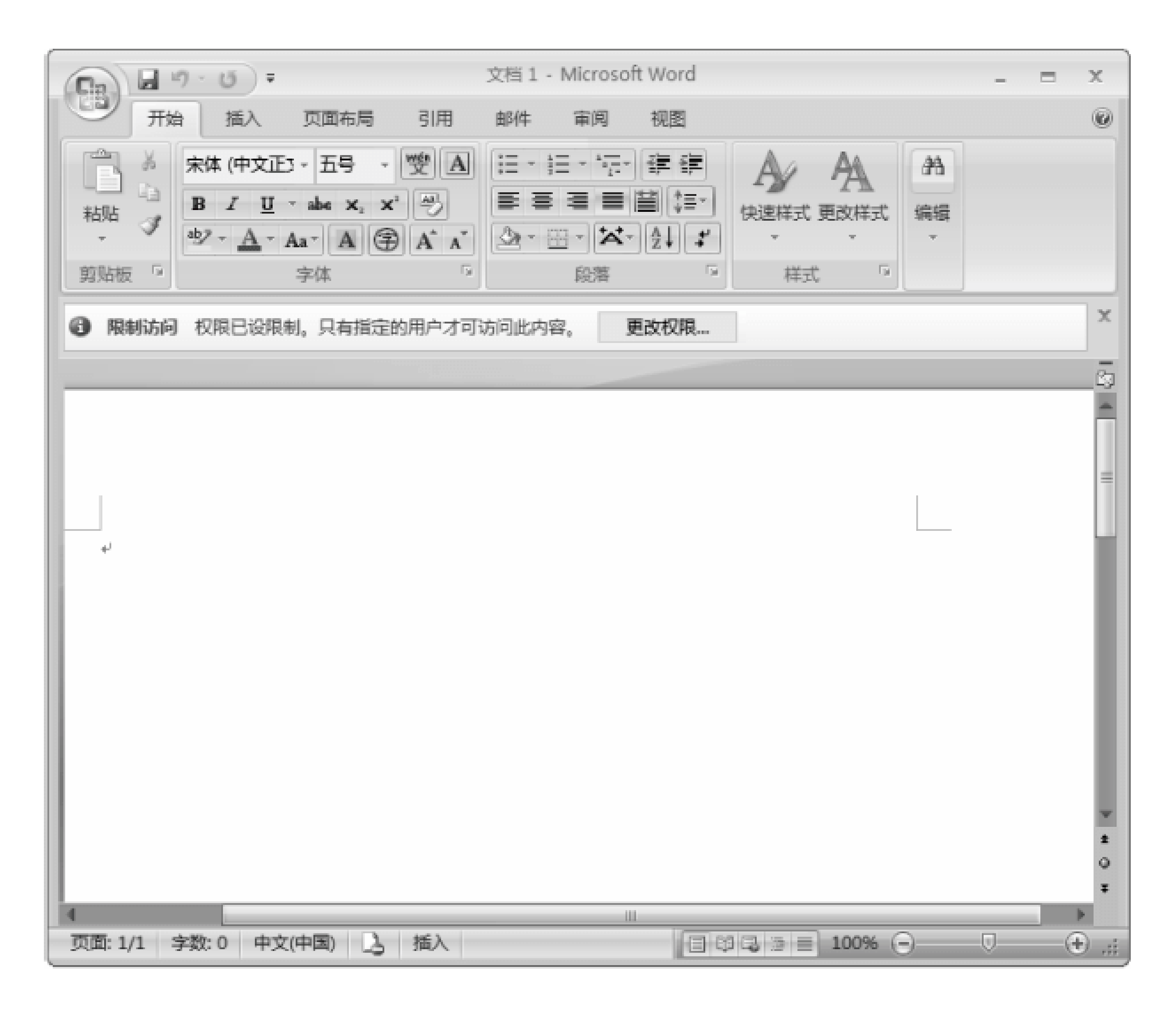


图 4-34　设置“限制访问”的文档

即修改权限设置。

4.3.2　打开被保护文档

用户打开被保护文档时，系统将要求登录.NET Passport 账户，从 Windows RM 证书服务器获取用户账户证书，根据文档的权限设置，用户即可获得相应的访问权限。

（1）用户打开受保护文档时，显示 Microsoft Office Word 对话框。单击“是”按钮，使用有效的 Hotmail 或 MSN 电子邮箱地址登录 Windows RM 证书服务器，申请用户账户证书即可。此过程与创建受保护文档完全相同，这里不再赘述。获得证书后，显示如图 4-35 所示的 Microsoft Office 对话框，提示“此文档的权限当前已被限制”。

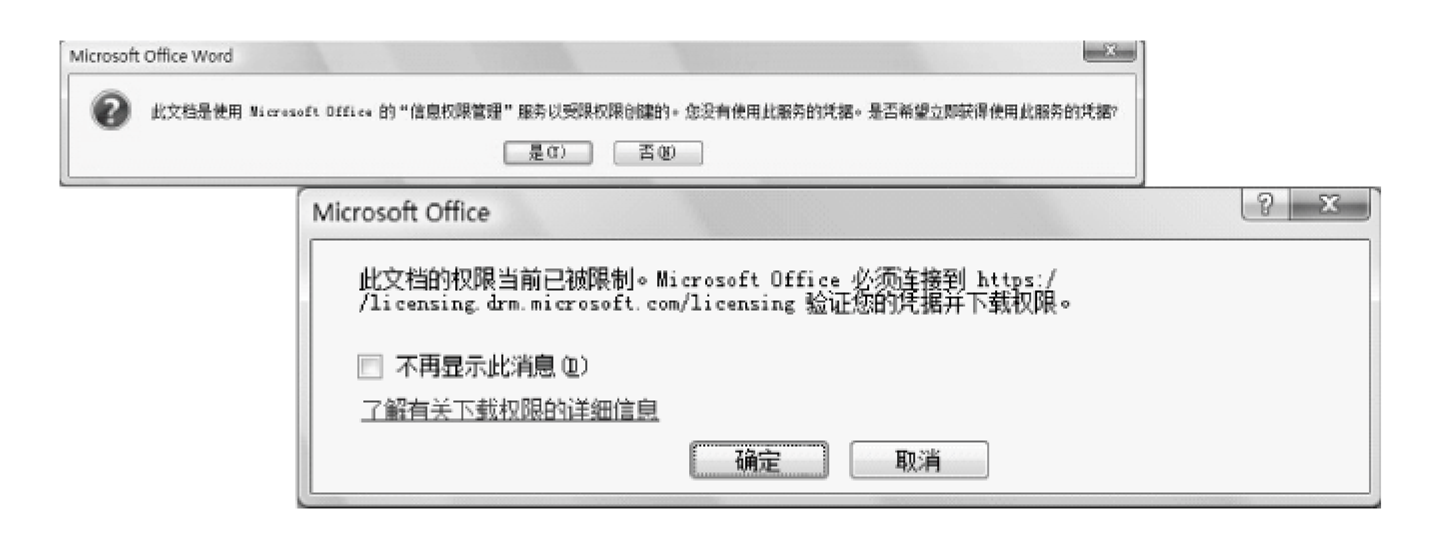


图 4-35　Microsoft Office 对话框

（2）单击“确定”按钮，Microsoft RM 服务器即可根据账户信息授予其相应访问权限。例如，当前登录账户的权限为“只读”，则打开文档后显示如图 4-36 所示的窗口，所有选项均为不可用状态。

4.3.3　请求权限

如果被保护文档的限制权限中，允许用户通过向所有者或具有完全控制权限的用户发

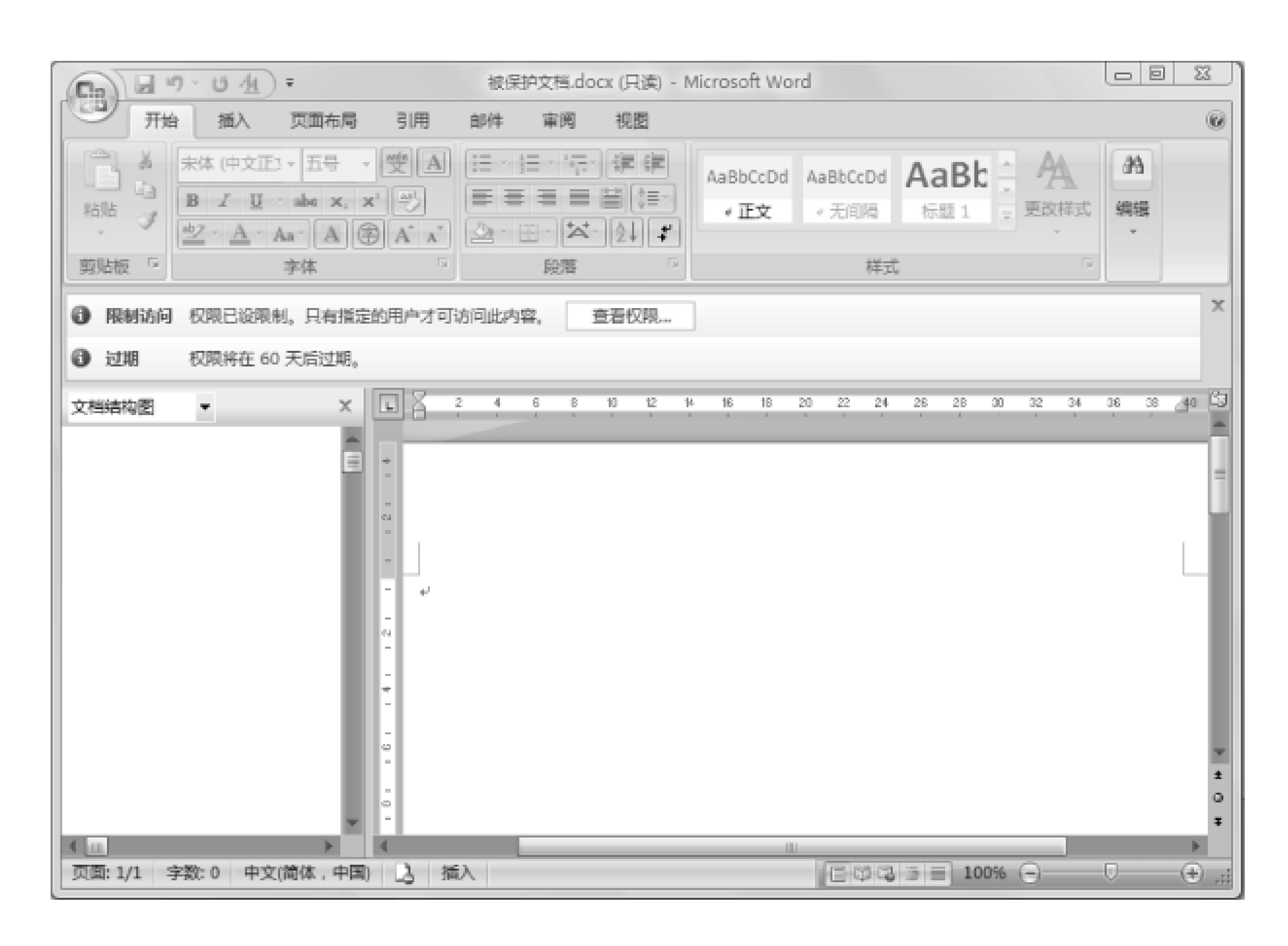


图 4-36 打开被保护的文档

送电子邮件，请求所需权限，则未被授权用户也可以通过该方式，获得被保护文档的相关权限。

未被授权用户打开被保护文档时，同样需要提供有效的.NET Passport 账户，申请 Windows RM 证书。完成后，显示如图 4-37 所示的 Microsoft Office Word 对话框。提示，当前用户没有打开文档的凭据。单击“是”按钮，启动电子邮件发送程序，以电子邮件的形式向管理员请求相应权限即可。收件人收到权限请求邮件之后，根据实际情况，核对是否授予其相应权限。如果是，则重新编辑被保护文档的权限限制即可。



图 4-37 Microsoft Office Word 对话框

4.3.4 知识链接：IRM

Microsoft Office 中的 IRM 为组织和信息工作者，控制他们自己的信息提供了又一种有益机制。IRM 是 Microsoft 开发的一种持久性的文件级保护技术，它允许信息工作者对有权访问和使用文档或电子邮件的人员加以指定，并且能够保护信息不受未经授权的打印、转发或复制。

IRM 对一种被称作 Windows 权限管理（Windows Rights Management）的关键 Windows 平台技术进行了扩展。权限管理是 Windows 的一种信息保护特性，它可以与应用程序相配合，对机密和敏感的企业信息加以保护——无论这些信息被发送到什么地方。作为对用户所提出的改善内容保护要求的响应，Microsoft 将权限管理设计为一个可扩展的平台，可以集成到 Office 以及各种第三方应用程序之中。

IRM 是一个策略工具，在对有权使用文档的人员和文档的使用目的进行控制的同时，允许用户对文档进行共享和通过电子邮件发送文档。因为 IRM 保护随着文件移动，所以该技术可以保护文档或者电子邮件，无论这些信息移动到什么地方，访问限制始终附加在信息之上；即便是文件被发送到了防火墙的外部也是如此。IRM 并不是一个安全特性，在用户被授予了有限制的权限之后，应用程序 UI 和对象模型还会应用剩余的其他限制，这些限制不能防止任何形式的滥用现象发生。

习题

1. 简述 AD RMS 服务在企业网络中的主要应用。
2. 在企业网络中部署 AD RMS 服务器之前应做好哪些准备工作?
3. 客户端如何应用 AD RMS 服务器上生成的权限策略模板?
4. 简述 IRM 和 AD RMS 有哪些异同。

实验:使用 IRM 保护机密文档

实验目的:

掌握如何通过 IRM 保护机密文档的安全。

实验内容:

企业网络中没有部署 AD RMS 服务器,使用.NET Passport 账户申请 RM 证书,保护机密文档的安全。

实验步骤:

(1) 打开需要保护的机密文档。

(2) 启动权限限制向导。

(3) 使用已有的 Windows Live 账户或.NET Passport 账户申请 RM 证书。

(4) 根据 Windows Live 账户或.NET Passport 账户赋予指定的用户账户查看权限,并设置文档的有效期为 7 天。

(5) 将使用 RM 证书保护的文档发送给对方。

(6) 对方用户使用被赋予权限的账户登录并获取 RM 证书,打开文档并验证是否可以编辑。

第 5 章 chapter 5

网络病毒防御

随着网络化应用程度的提高,有效阻止网络病毒入侵已经成为网络安全的一个重要课题。网络病毒将直接影响网络的正常运行,轻则降低响应速度,影响工作效率,重则服务器死机,甚至网络瘫痪。如今大多数病毒都是通过网络传播的,而且传播速度极快,大大增加了管理员处理的难度。因此,在局域网中,通常部署统一的网络病毒防御系统,借助防病毒服务器自动管理所有网络客户端的病毒查杀、病毒库升级等工作。

5.1 网络病毒防御规划

近几年来,网络病毒、木马、恶意软件、间谍程序已经成为影响网络安全的主要因素。网络攻击的“商业性”特征更加突出,企业网络中的重要服务器、关键数据往往是入侵者袭击的首要目标。

5.1.1 案例情景

目前,该企业网络中的大部分服务器和客户端都部署了杀毒软件和病毒防火墙,主要包括 Symantec、瑞星和金山毒霸等。这些防病毒措施虽然可以阻止大部分常规网络病毒的入侵,但是为了确保服务器杀毒软件病毒特征库的时效性,管理员需要经常检查杀毒软件的升级情况,非常麻烦。由于杀毒软件类别和型号各不相同,很难实现统一管理,操作起来非常麻烦。

大部分客户端计算机都已经安装了杀毒软件,但能够按时升级病毒特征库和执行病毒扫描的却很少,通常都是由于杀毒软件的版本过于陈旧,未能阻止和查杀入侵系统的新型病毒,最终导致系统崩溃或感染到网络中的其他计算机。总而言之,客户端计算机上的杀毒软件利用效率不高。

5.1.2 项目需求

随着计算机病毒的不断演变和升级,原有的分散式防病毒措施已经很难奏效。虽然管理员可以确保服务器上防病毒系统的安全性和有效性,但通过客户端计算机入侵的网络病毒,同样会感染到网络中的其他计算机,甚至是服务器,这也是现有安全防御体系频频失守的重要因素。

切实有效的防病毒系统不仅是检测和清除病毒,还应加强对病毒的防护工作。因此,在

网络中不仅要部署被动防御体系(防病毒系统)还要采用主动防御机制(防火墙、安全策略、漏洞修复等),将病毒隔离在网络大门之外。通过管理控制台统一部署防病毒系统,保证不出现防病毒漏洞。因此,远程安装、集中管理、统一防病毒策略成为校园网中防病毒产品的重要需求。

5.1.3　解决方案

鉴于该网络的需求以及当前计算机病毒的特征,可以从如下方面出发,打造计算机病毒防御体系。

(1) 构建控管中心集中管理架构。保证网络中的所有客户端计算机、服务器可以从管理系统中及时得到更新,同时系统管理人员可以在任何时间、任何地点通过浏览器对整个防毒系统进行管理,使整个系统中任何一个节点都可以被系统管理人员随时管理,保证整个防毒系统有效、及时地拦截病毒。

(2) 构建全方位、多层次的防毒体系。结合企业实际网络防毒需求,构建了多层次病毒防线,分别是网络层防毒、邮件网关防毒、Web 网关防毒、群件防毒、应用服务器防毒、客户端防毒,保证斩断病毒可以传播、寄生的每一个节点,实现病毒的全面布控。

(3) 构建高效的网关防毒子系统。网关防毒是最重要的一道防线,一方面消除外来邮件 SMTP、POP3 病毒的威胁;另一方面消除通过 HTTP、FTP 等应用的病毒风险,同时对邮件中的关键字、垃圾邮件进行阻挡,有效阻断病毒最主要传播途径。

(4) 构建高效的网络层防毒子系统。校园中网络病毒的防范是最重要的防范工作,通过在网络接口和重要安全区域部署网络病毒系统,在网络层全面消除外来病毒的威胁,使得网络病毒不再肆意传播,同时结合病毒所利用的传播途径,结合安全策略进行主动防御。

目前各大网络安全厂商主推的网络防病毒系统,非常适合网络病毒安全的防御系统,例如 Symantec、瑞星等。网络防病毒系统主要由服务器和客户端两部分组成。主要特点就是客户端可以直接通过局域网从服务器获得最新的病毒库升级文件,并且管理员可以通过防病毒服务器客户端监控功能,及时了解客户端的运行情况,以便统一管理和部署。因此,部署企业杀毒软件系统不仅可以节省整个网络的带宽开销,还可以提高网络安全性。图 5-1 所示的是大多数企业杀毒软件的运行模式。

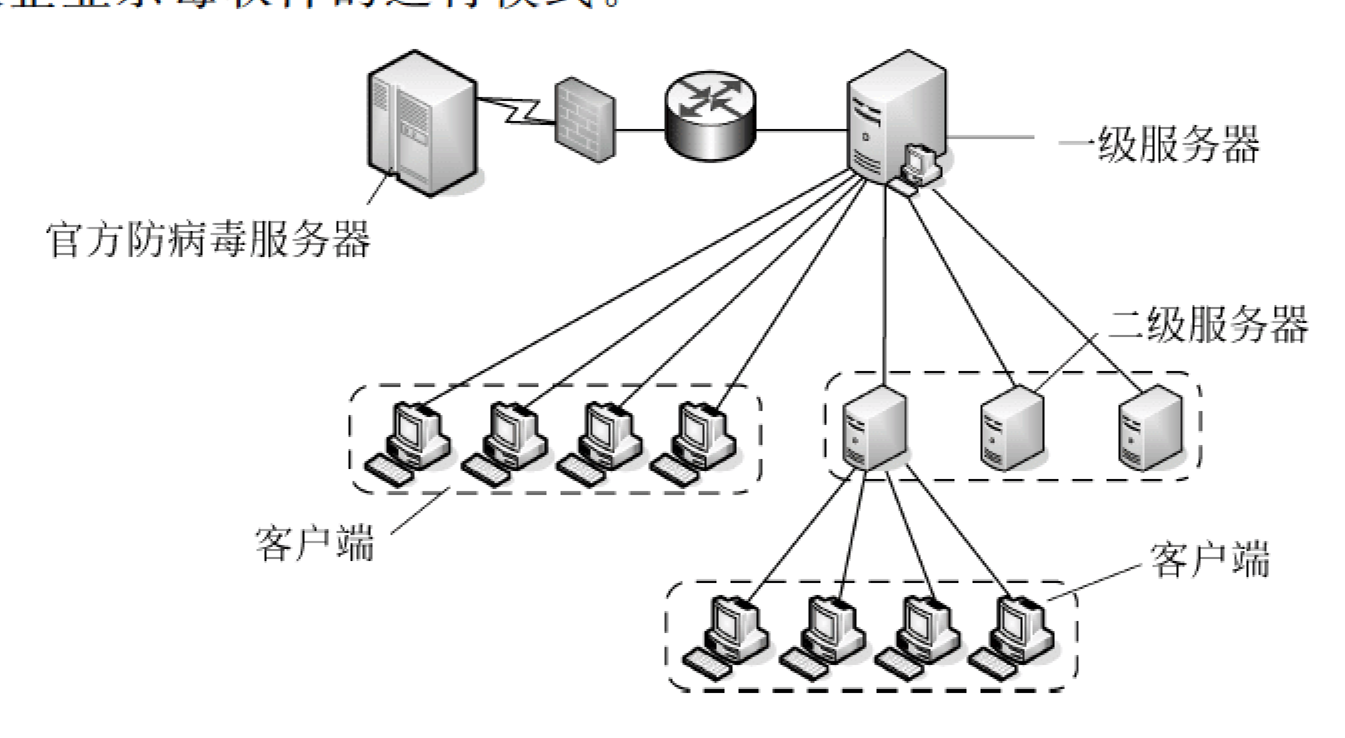


图 5-1　网络防病毒系统

企业网络杀毒软件系统中的服务器端是指安装服务器管理软件的计算机,可以直接登录杀毒软件官方升级服务器,快速下载最新病毒库文件。管理员可以通过服务器端对下属的二级服务器、客户端等进行统一管理,如分发升级文件、接收客户端病毒报警、实时状态监控等。另外,服务器端通常都集成适用于各种版本操作系统的客户端安装程序,管理员可以直接通过局域网安装客户端,免去一一安装的麻烦。

客户端是指接受网络防病毒服务器管理的所有计算机,必须安装与服务器端配套的杀毒软件,并接受服务器的管理。客户端既可手动连接到局域网防病毒服务器更新病毒库,也可以指定为自动接收来自服务器的病毒库文件。

5.2 病毒概述

随着网络功能的不断拓展,信息安全性的要求也越来越高,以至于国家信息安全部门不得不在电视、广播、网络等各大媒体提醒用户,或发布最新的安全警示。计算机病毒是威胁网络安全的主要方面,其实大家对计算机病毒并不陌生,即使自己没有感染过也会听到或看到过,尤其是经过近几年"冲击波"、"振荡波"、"灰鸽子"、"熊猫烧香"等网络病毒的肆虐之后,谈起计算机病毒更是让人心惊胆战。

5.2.1 计算机病毒

从广义上定义,凡能够引起计算机故障,破坏计算机数据的程序统称为计算机病毒。根据该定义,逻辑炸弹、蠕虫等均可称为计算机病毒。根据《中华人民共和国计算机信息系统安全保护条例》,第二十八条中明确指出:"计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。"计算机病毒必须满足两个条件。①必须能自动执行;②必须能自动复制。

1. 计算机病毒的特征

计算机病毒通常具备传染性、隐蔽性、潜伏性、欺骗性、表现性、破坏性 6 大特性。

(1) 传染性:计算机病毒可通过各种可能的渠道,如软盘、盗版光盘、计算机网络、电子邮件去传染其他的计算机。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

(2) 隐蔽性:病毒一般是具有很高编写技巧而且短小精悍的程序。通常附在正常程序中或操作系统中较隐蔽的地方,也有很多文件以隐藏形式出现,目的是不让用户发现它的存在。

(3) 潜伏性:有一些病毒在感染系统之后并不立即发作,而是要潜伏一段时期,等待触发条件满足之后才发作。

(4) 欺骗性:病毒往往会有一些很好看的图标,很好听的名称,邮件病毒会有一些很有诱惑力的标题,使用户认为它是正常的程序,从而点击运行,执行病毒程序。

(5) 表现性:计算机病毒进入系统都会对系统有不同程度的影响,一般带有个人情绪的病毒或恶作剧程序发作的时候表现特征明显一些。

(6) 破坏性:所有的计算机病毒都存在一个共同的危害,即降低计算机系统的工作效率,占用系统资源,其具体情况取决于计算机病毒设计者的目的。

2. 新时代病毒的特性

近几年,危害严重的计算机病毒通常具有如下共同特点。

(1) 与经济利益挂钩:各种盗取账号的木马、后门程序等新型病毒已经成为某些公司非法敛财的工具。病毒背后的巨大的灰色产业链给整个互联网带来了更加严峻的考验。

(2) "网页挂马"与 ARP 欺骗危害加剧:近几年来,网页挂马成爆炸式增长,而且挂马程序使用的木马隐蔽性越来越高,致使大多数管理员很难发现。ARP 攻击是局域网中最常见的攻击方式之一,其最新表现方式是同其他挂马程序配合应用,达到攻击的目的。

(3) 团队化运作方式:伴随着安全厂商对病毒的剿杀,病毒制作者开始想方设法逃避杀毒软件的追杀,甚至从技术的角度对杀毒软件进行攻击。首先,有专人负责开发病毒程序,再由专人将其散播到网站或目标用户的计算机,最后将窃取到的信息反馈到处理中心,处理中心则根据用户信息的价值进行相应的处理。

(4) 变种数量成为病毒危害性的新标准:通常情况下,一种新型的计算机病毒的破坏力并不可怕,可怕的是随之而来的各种变种。一种病毒衍生出多种病毒,通过更多的手段传播,迫使更多的人参与,被感染的用户也就越来越多。

5.2.2 木马

特洛伊木马(简称木马),英文名称 Trojan Horse。木马是指那些表面上是有用的软件而实际目的却是危害计算机安全并导致严重破坏的计算机程序。木马是一种基于远程控制的黑客工具,典型客户端/服务器端(C/S)控制模式,客户端也称为控制端。木马通常具有如下 3 个特性。

(1) 隐蔽性:木马的设计者为了防止木马被发现,采用多种手段隐藏木马,这样服务端即使发现感染了木马,也难以确定其具体位置。

(2) 非授权性:控制端与服务端连接后,控制端将窃取到服务端的操作权限,如修改文件,修改注册表等,以窃取服务端的信息,例如个人账户、密码、数据库信息等。

(3) 破坏性:木马的发作要在远程服务端的计算机运行服务程序,一旦发作,自动设置后门,定时地发送该计算机用户的隐私到木马程序指定的地址,客户端可以通过预设的端口和服务端连接,可任意控制此计算机,进行文件删除、复制、修改密码等操作。

木马与病毒的重大区别是木马不具传染性,它并不能像病毒那样自我复制,也并不"主动"地去感染其他文件,主要通过将自身伪装起来,吸引计算机用户下载执行。

木马中包含能够在触发时导致数据丢失甚至被窃的恶意代码,要使木马传播,必须在计算机上有效地启用这些程序,例如打开电子邮件附件或者将木马捆绑在软件中放到网络上吸引浏览者下载执行等。

目前,木马一般主要以窃取用户相关信息为主要目的。相对病毒而言,可以简单地说,病毒破坏计算机使用者的信息,而木马窃取计算机使用者的信息。

5.2.3 蠕虫病毒

蠕虫是设计用来将自己从一台计算机复制到另一台计算机,并执行预定操作功能的程序代码,蠕虫可以自动执行,同时可以自我复制,系统一旦感染蠕虫,蠕虫即可自行传播。蠕

虫是一种通过网络传播的恶性病毒,它具有病毒的一些共性,如传播性、隐蔽性、破坏性等,同时也具有自己的一些特征,如不利用文件寄生(有的只存在于内存中)、使网络造成拒绝服务、与黑客技术相结合等。例如,蠕虫可向电子邮件地址簿中的所有联系人发送自己的副本,那些联系人的计算机也将执行同样的操作,结果造成多米诺效应(网络通信负担沉重),使计算机和整个 Internet 的速度减慢。

普通病毒的传染能力主要是针对计算机内的文件系统而言,而蠕虫病毒的传染目标是局域网和互联网内的所有计算机。系统一旦感染蠕虫,蠕虫即可自行传播,将自己从一台计算机复制到另一台计算机。因而在产生的破坏性上,蠕虫病毒不是普通病毒所能比拟的,网络的发展使得蠕虫可以在短短的时间内蔓延至整个网络,造成网络瘫痪。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等,都是蠕虫传播的良好途径。蠕虫病毒可以在几个小时内蔓延全球,而且蠕虫的主动攻击性和突然爆发性使网络管理员手足无措。同时,蠕虫会占用内存或网络带宽,从而可能导致网络和计算机崩溃。蠕虫的传播不必通过“宿主”程序或文件,它的危害远比普通病毒大。典型的蠕虫病毒有尼姆达、震荡波等。

蠕虫病毒主要通过 3 种途径传播:系统漏洞、聊天软件和电子邮件。

5.2.4 网页病毒

网页病毒主要是利用软件或系统操作平台等的安全漏洞,通过执行嵌入在网页 HTML 超文本标记语言内的 Java Applet 小应用程序、JavaScript 脚本语言程序、ActiveX 控件网络交互技术支持可自动执行的代码程序,以强行修改用户操作系统的注册表设置及系统实用配置程序,或非法控制系统资源盗取用户文件,或恶意删除硬盘文件、格式化硬盘等。

网页病毒完全不受计算机用户控制,一旦浏览含有该病毒的网页,在没有防护措施的情况下,立即被感染,给计算机用户的系统带来一般性的、轻度性的、严重的、恶性的等不同程度的破坏,同时访问网页的速度变慢,甚至导致损失惨重无法弥补。

根据目前互联网上流行的常见网页病毒的作用对象及表现特征,将其归纳为以下两大类。

第一类:通过 JavaScript、Applet、ActiveX 编辑的脚本程序修改 IE 浏览器,可以造成如下后果。

(1) 默认主页、首页、微软主页被修改。

(2) 主页设置被屏蔽锁定,且设置选项无效不可改回。

(3) 默认的 IE 搜索引擎被修改。

(4) IE 标题栏被添加非法信息。

(5) 鼠标右键菜单被添加非法网站广告链接。

(6) 鼠标右键弹出菜单功能被禁用、失常。

(7) IE 收藏夹被强行添加非法网站的地址链接。

(8) 在 IE 工具栏非法添加按钮。

(9) 锁定地址下拉菜单及其添加文字信息。

(10) IE 菜单“查看”下的“源文件”被禁用。

第二类:通过 JavaScript、Applet、ActiveX 编辑的脚本程序修改用户操作系统,可以造

成如下后果。

(1) 开机出现对话框。

(2) 系统正常启动后,IE被锁定网址自动调用打开。

(3) 格式化硬盘。

(4) 全方位侵害封杀系统,最后导致瘫痪崩溃。

(5) 非法读取或盗取用户文件。

(6) 锁定、禁用注册表。

(7) 注册表被锁定禁用之后,编辑.reg注册表文件打开方式错乱。

(8) 添加广告。

(9) 启动后首页被再次修改。

(10) 更改"我的电脑"下的一系列文件夹名称。

5.2.5 恶意软件

中国互联网协会对恶意软件的定义是:在未明确提示用户或未经用户许可的情况下,在用户计算机或其他终端上安装运行,侵害用户合法权益的软件,但不包含我国法律法规规定的计算机病毒。具有下列特征之一的软件可以被认为是恶意软件。

(1) 强制安装:指未明确提示用户或未经用户许可,在用户计算机或其他终端上安装软件的行为。

(2) 难以卸载:指未提供通用的卸载方式,或在不受其他软件影响、人为破坏的情况下,卸载后仍然有活动程序的行为。

(3) 浏览器劫持:指未经用户许可,修改用户浏览器或其他相关设置,迫使用户访问特定网站或导致用户无法正常上网的行为。

(4) 广告弹出:指未明确提示用户或未经用户许可,利用安装在用户计算机或其他终端上的软件弹出广告的行为。

(5) 恶意收集用户信息:指未明确提示用户或未经用户许可,恶意收集用户信息的行为。

(6) 恶意卸载:指未明确提示用户,未经用户许可,或误导、欺骗用户卸载其他软件的行为。

(7) 恶意捆绑:指在软件中捆绑已被认定为恶意软件的行为。

(8) 行为记录:行为记录软件是指未经用户许可,窃取并分析用户隐私数据,记录用户计算机使用习惯、网络浏览习惯等个人行为的软件。

(9) 其他侵害用户软件安装、使用和卸载知情权、选择权的恶意行为。

5.2.6 中毒症状

计算机病毒是一段程序代码,虽然病毒可能隐藏得很好,但也会留下许多痕迹。通过对这些蛛丝马迹的判别,就可以发现已经存在的计算机病毒。计算机用户可以根据以下现象判断自己的操作系统是否已经感染了病毒。

(1) 系统运行速度减慢。

(2) 系统经常无故死机。

(3) 系统经常无故重新启动。

(4) 系统文件长度发生变化。

(5) 系统提示内存不足。

(6) 磁盘存储空间容量异常减少。

(7) 系统引导速度变慢。

(8) 丢失文件或者文件损坏。

(9) 计算机扬声器异常声响。

(10) 屏幕出现异常显示。

(11) 磁盘卷标自动发生变化。

(12) 硬盘丢失。

(13) 磁盘访问异常(无工作时硬盘指示灯狂闪)。

(14) 键盘输入异常。

(15) 文件的属性(日期、时间等)发生变化。

(16) 无法正常读取、打开文件。

(17) 异常要求用户输入密码。

(18) 在没有编辑过宏的前提下 Word 或者 Excel 提示执行“宏”。

(19) 有未知程序常驻内存。

(20) 系统出现大量来历不明的文件。

(21) 系统自动执行某些操作。

(22) 开机运行异常程序。

(23) 网络流量异常。

(24) 任务管理器中出现可疑进程。

(25) 系统服务中的奇怪项目。

(26) 访问网络速度极慢。

(27) 系统中打开许多端口。

(28) 收到包含奇怪附件的电子邮件。打开附件后,出现对话框或系统性能突然降低。

(29) 防病毒程序被无端禁用,并且无法重新启动。

(30) 无法在计算机上安装防病毒程序,或安装的防病毒程序无法运行。

(31) 屏幕上出现奇怪的对话框或消息框。桌面上出现的新图标不是由操作者放置的,或者与最近安装的任何程序都无关。

(32) 由于某些关键的系统文件丢失,Windows 无法启动,然后出现错误消息并列出这些丢失的文件。

(33) 防病毒软件提示存在病毒。

(34) 浏览器设置被强行修改。

(35) 自动弹出广告窗口。

(36) 自动打开网站。

当计算机出现如上所述的情况时,系统就有可能感染了病毒,建议立即升级病毒库,启动病毒查杀软件,查杀可能存在的病毒。

5.2.7　传播途径

计算机病毒具有自我复制和传播的特点，从计算机病毒的传播机理分析可知，只要是能够进行数据交换的介质都有可能成为计算机病毒的传播途径。传统的手工传播计算机病毒的方式与现在通过 Internet 传播相比速度要慢得多。

1. 移动存储设备

可移动设备例如软盘、光盘、磁带、U 盘等，盗版光盘上的软件和游戏及非法复制也是目前传播计算机病毒的主要途径之一。随着大容量可移动存储设备如 Zip 盘、可擦写光盘、磁光盘(MO)等的普遍使用，这些存储介质也将成为计算机病毒寄生的场所。

硬盘是数据的主要存储介质，因此也是计算机病毒感染的重灾区。硬盘传播计算机病毒的途径主要是：硬盘向软盘上复制带毒文件，带毒情况下格式化软盘，向光盘上刻录带毒文件，硬盘之间的数据复制，以及将带毒文件发送至其他地方等。在移动存储设备中，U 盘是使用最广泛移动最频繁的存储介质，因此也成了计算机病毒寄生的"温床"。

2. 计算机网络

现代信息技术的巨大进步已使空间距离不再遥远，"相隔天涯，如在咫尺"，但也为计算机病毒的传播提供了新的"高速公路"。计算机病毒可以附着在正常文件中通过网络进入一个又一个系统，而且病毒在计算机网络环境中的传播速度非常快。

3. 点对点通信系统和无线网络

目前，这种传播途径还不是十分广泛，但预计在未来的信息时代，这种途径很可能与网络传播途径成为病毒扩散的两大"时尚渠道"。

4. 电子邮件

现在很多蠕虫病毒都是通过邮件传播的，一般是在邮件的附件中夹带着病毒文件，用户一旦双击运行附件就会中毒。

5.3　SEP 企业版的安装

SEP Manager 类似于 Symantec AntiVirus 企业版中的系统中心，主要用于管理 SEP 服务器和客户端，直接从光盘安装即可。SEP Manager 引进了数据库管理技术，最多可以支持超过 5000 个端点的网络环境，管理员可以通过创建不同的服务器组，实现网络负载均衡。

5.3.1　安装要求

新一代 Symantec 计算机网络安全防御系统对目标计算机硬件和软件的要求更加严格，除满足最低需求外，目标计算机的用户账户还必须拥有远程登录和管理客户机的权限，以便实现远程部署和管理。

1. 硬件需求

安装 SEP Manager 的基本硬件需求如表 5-1 所示，硬件性能的高低将直接影响到服务器的稳定性和可以支持的客户端数量。

表 5-1 SEP Manager 基本硬件需求

组 件	x86	x64
处理器	1GHz Intel Pentium Ⅲ	Intel EM64T 的 Intel Xeon 和 Intel Pentium Ⅳ 处理器、AMD 64 位 Opteron 和 Athlon 处理器，不支持 Itanium 处理器
内存	1GB(建议使用 2GB)	1GB(建议使用 2GB)
硬盘	2GB(建议使用 4GB)	2GB(建议使用 4GB)
显示器	Super VGA(1024×768) 或更高分辨率的视频适配器和显示器	Super VGA(1024×768) 或更高分辨率的视频适配器和显示器

2. 系统和软件需求

SEP Manager 支持以下操作系统。

(1) Windows 2000 Server SP3 或更高版本。

(2) Windows XP Professional(Service Pack 1)或更高版本。

(3) Windows Server 2003 各种版本(64 位版本必须集成 SP1 或更高版本系统补丁)。

(4) x64 Windows Server 2003 服务器群集。

(5) Windows Server 2008 各种版本(Server Core 除外)。

(6) x64 Windows Essential Business Server 2008 系列和 Windows Small Business Server 2008 系列。

注意：*如果要为 SEP Manager 服务器使用 Microsoft 群集服务，则必须在本地卷上安装 SEP Manager 服务器。*

安装 SEP Manager 的计算机必须满足下列最低软件要求。

(1) 安装和启用 IIS 5.0 或更高版本，如果使用 IIS 7.0，则必须安装 CGI、ASP.NET 以及 IIS 6.0 管理兼容性等组件。

(2) Internet Explorer 6.0 或更高版本。

(3) 使用静态 IP 地址。

(4) Microsoft SQL 2000/2005 数据库服务器(可选)。

3. 用户权限需求

若要安装 Symantec 客户端软件，用户必须对客户端计算机或 Windows 域具有管理员权限，并以管理员的身份登录。Symantec 软件安装程序会在计算机上启动另一个安装程序，以便创建和启动服务并修改注册表。

如果不想为用户提供其计算机的管理权限，可以使用“推式部署向导”远程安装 Symantec 客户端。要运行“推式部署向导”，必须具有对安装该程序的计算机的本地管理权限。

如果是用 Active Directory 管理计算机，可以创建“组策略”，该策略将提供安装 Symantec 软件所必需的用户权限。

5.3.2 安装 SEP Manager

安装 SEP Manager 之前必须确保已经安装并启动了 IIS 服务，数据库服务器是可选的，如果网络客户端数量不超过 1000 个，完全可以使用 SEP 内置的嵌入式数据库，如果客户端

数量较多，则建议安装独立的 SQL Server 数据库，并建立相应的数据库实例。

（1）插入安装光盘，如果安装程序未自动启动，则可以双击根目录下的 Setup.exe 文件启动安装程序，显示如图 5-2 所示的“Symantec Endpoint Protection 安装程序”对话框。

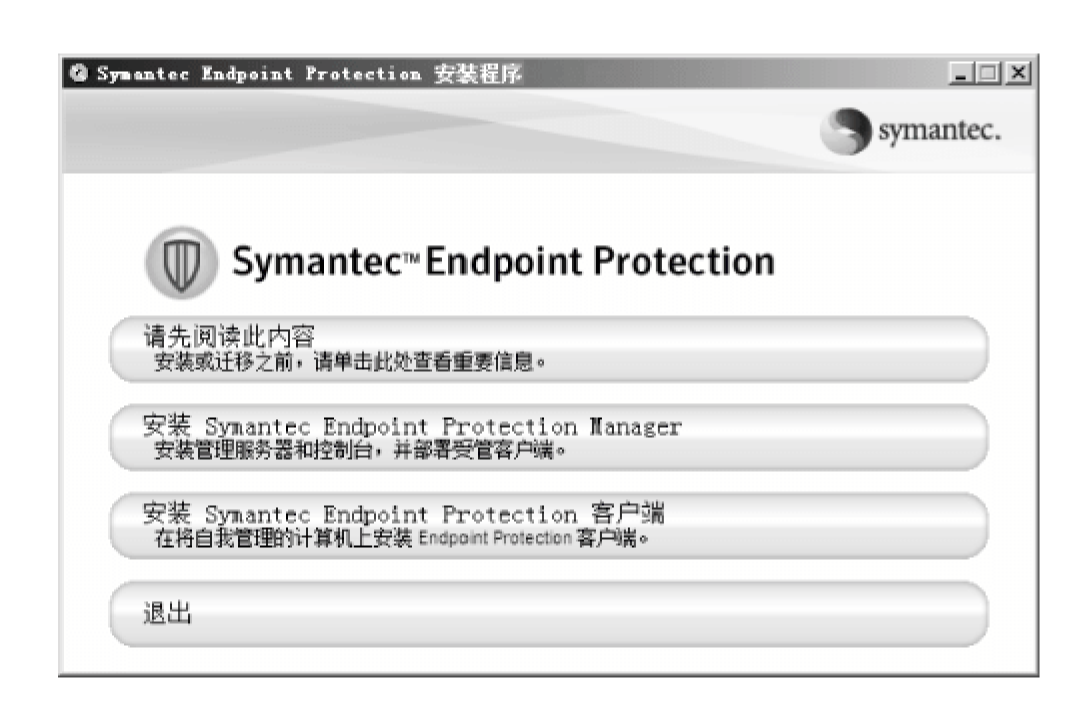


图 5-2 “Symantec Endpoint Protection 安装程序”对话框

（2）单击“安装 Symantec Endpoint Protection Manager”按钮，启动 SEP Manager 安装向导，直接单击“下一步”按钮，选中“我接受该许可证协议中的条款”单选按钮即可。继续单击“下一步”按钮，显示如图 5-3 所示的“目标文件夹”对话框，单击“更改”按钮可以重新选择安装目录，建议接受默认安装路径。

（3）单击“下一步”按钮，显示如图 5-4 所示的“选择网站”对话框。若要在该服务器上让 SEP Manager IIS Web 和原有 Web 站点同时运行，则选中“使用默认 Web 站点”单选按钮；若要将 SEP Manager IIS Web 配置为当前服务器上唯一的 Web 站点，则选中“创建自定义网站”单选按钮。为了提高 Symantec 服务器自身的安全性，建议选中“创建自定义网站”单选按钮。



图 5-3 “目标文件夹”对话框



图 5-4 “选择网站”对话框

（4）单击“下一步”按钮，显示“准备安装程序”对话框，提示安装向导已经准备就绪。单击“安装”按钮，即可开始安装，需要等待几分钟时间。安装完成后，单击“完成”按钮，即可完成 SEP Manager 的安装，并自动启动 SEP Manager 配置向导。

5.3.3 配置 SEP Manager

安装 SEP Manager 之后，还需要根据需要进行相应配置，包括创建服务器组、设置站点

名称、管理员密码、客户端安装方式以及制作客户端安装包等。默认情况下，关闭 Symantec Endpoint Protection 安装向导后将自动启动“管理服务器配置向导”，如果没有启动也可按照如下方法打开并配置。

（1）依次选择“开始”→“所有程序”→Symantec Endpoint Protection Manager→“管理服务器配置向导”选项，默认显示“欢迎使用管理服务器配置向导”对话框。本例中需要部署支持大约 500 个客户端的服务器，因此选中“高级”单选按钮。单击“下一步”按钮，指定该管理服务器管理的客户端数量，根据实际情况选择即可，本例选中“500 到 1000 台”单选按钮，如图 5-5 所示。

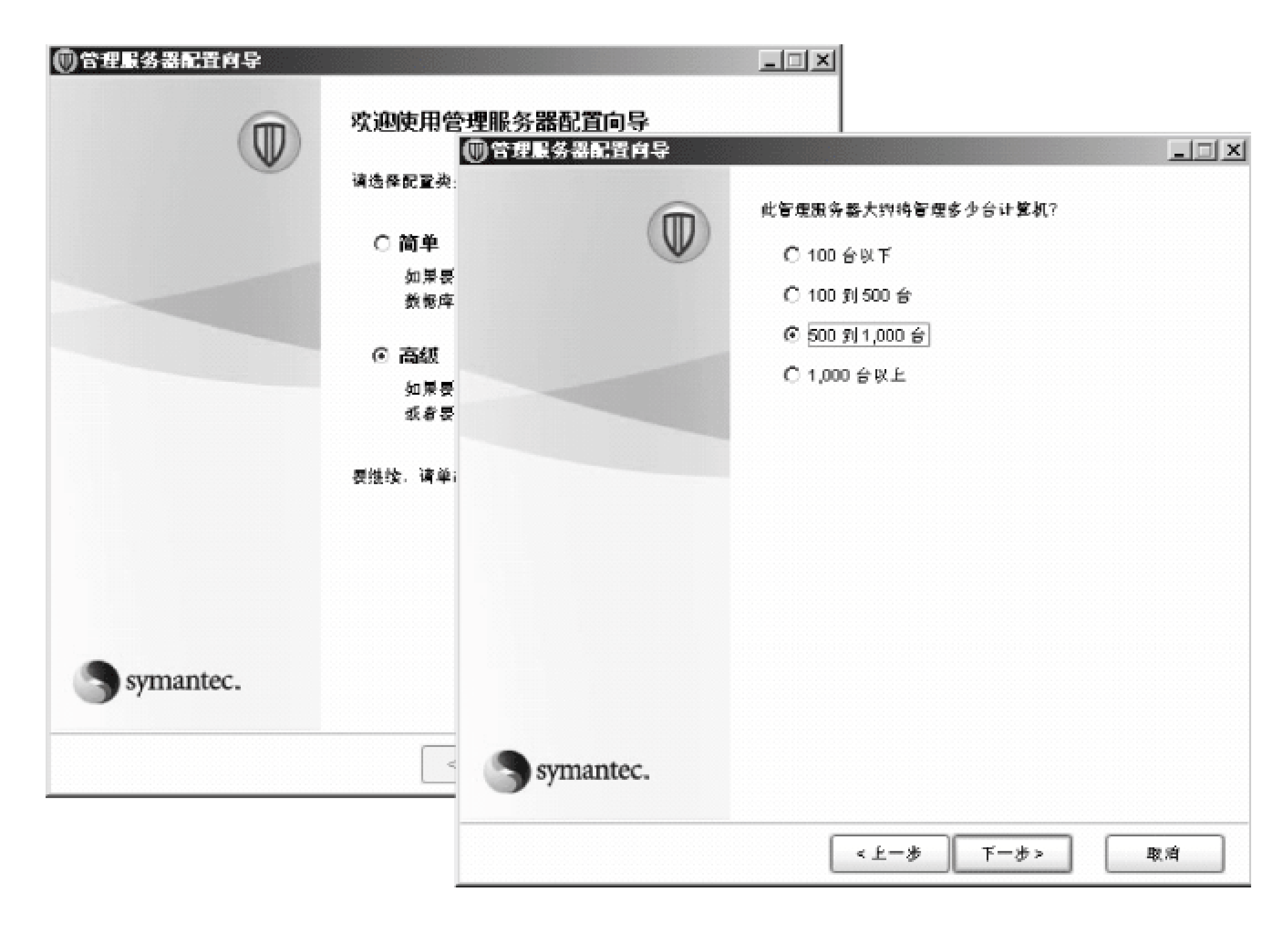


图 5-5　指定客户端数量

（2）单击“下一步”按钮，选中“安装我的第一个站点”单选按钮即可。无论使用单点管理模式还是使用服务器群集模式，都必须先安装并配置第一个管理服务器站点。单击“下一步”按钮，指定管理服务器名称和通信端口。在“服务器名”文本框中输入 Symantec 管理服务器的名称，便于客户端查找和确认；“服务器端口”和“Web 控制台端口”均保持默认即可。单击“下一步”按钮，设置站点名称，在“站点名”文本框中输入适当名称即可，如 SEP，如图 5-6 所示。

（3）单击“下一步”按钮，设置加密密码。在 SEP 安全防御系统中，管理服务器和客户端之间的通信均是被加密的，以确保传输过程中的安全。单击“下一步”按钮，选择希望适用的数据库类型，本例为“嵌入式数据库”。如果客户端数量不超过 5000 个，则建议选择默认的“嵌入式数据库”，以避免不必要的兼容性问题。如果希望实现服务器群集，则必须选中 Microsoft SQL Server 单选按钮。单击“下一步”按钮，创建系统管理员账户，默认账户名称为 admin，在“密码”和“确认密码”文本框中输入管理员账户的登录密码即可，如图 5-7 所示。

注意：*必须妥善保管此密码。创建数据库之后，将不能更改或恢复密码。当没有可还原的备份数据库时，必须输入此密码，才能进行灾难恢复。*

（4）单击“下一步”按钮，开始创建嵌入式数据库。完成后会提示此向导并不会在本地计算机上安装 SEP 客户端。如果选中“是”单选按钮，则单击“完成”按钮将自动启动“迁移和部署向导”，以便完成客户端远程安装包的创建等工作。

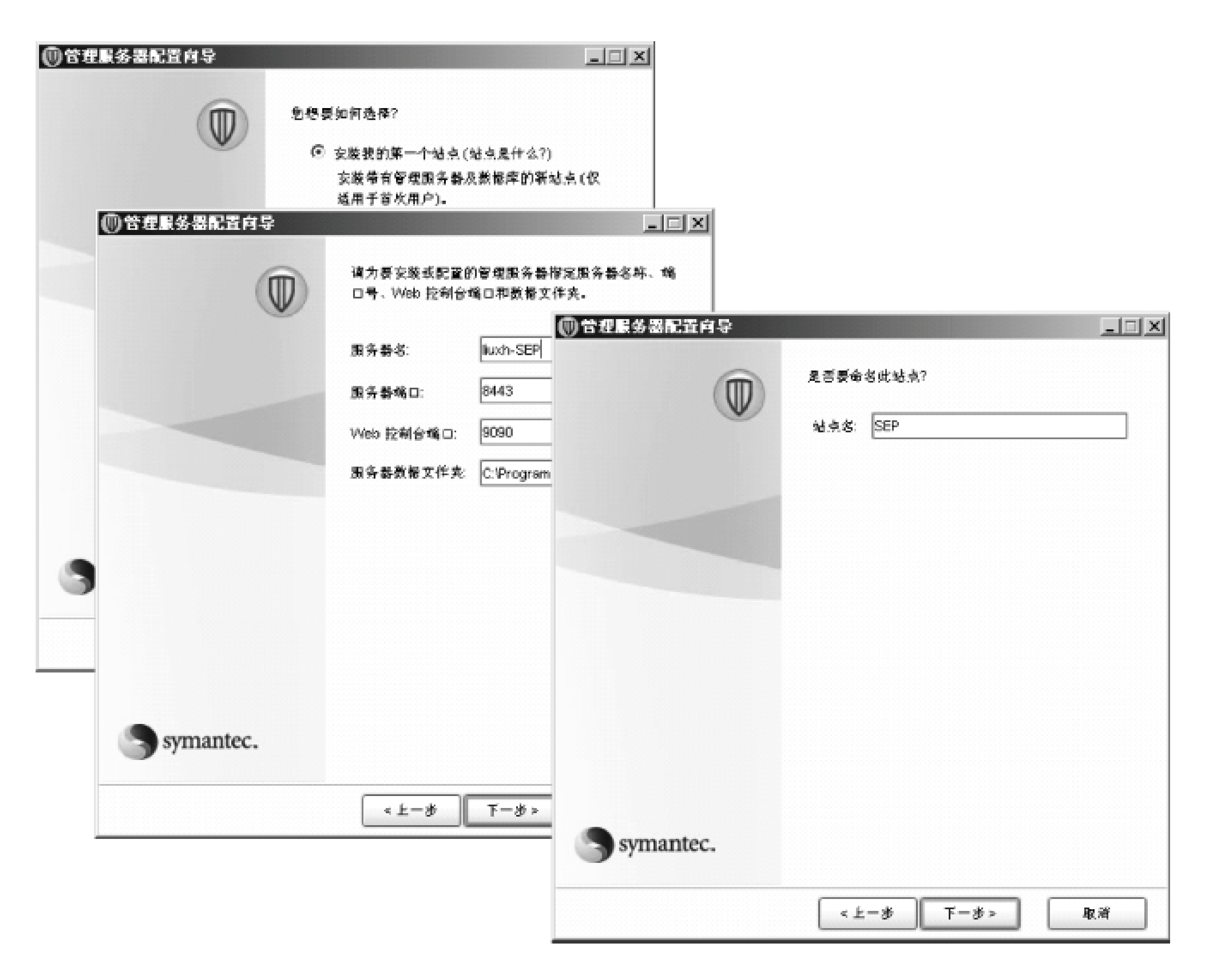


图 5-6　设置服务器名称和站点名

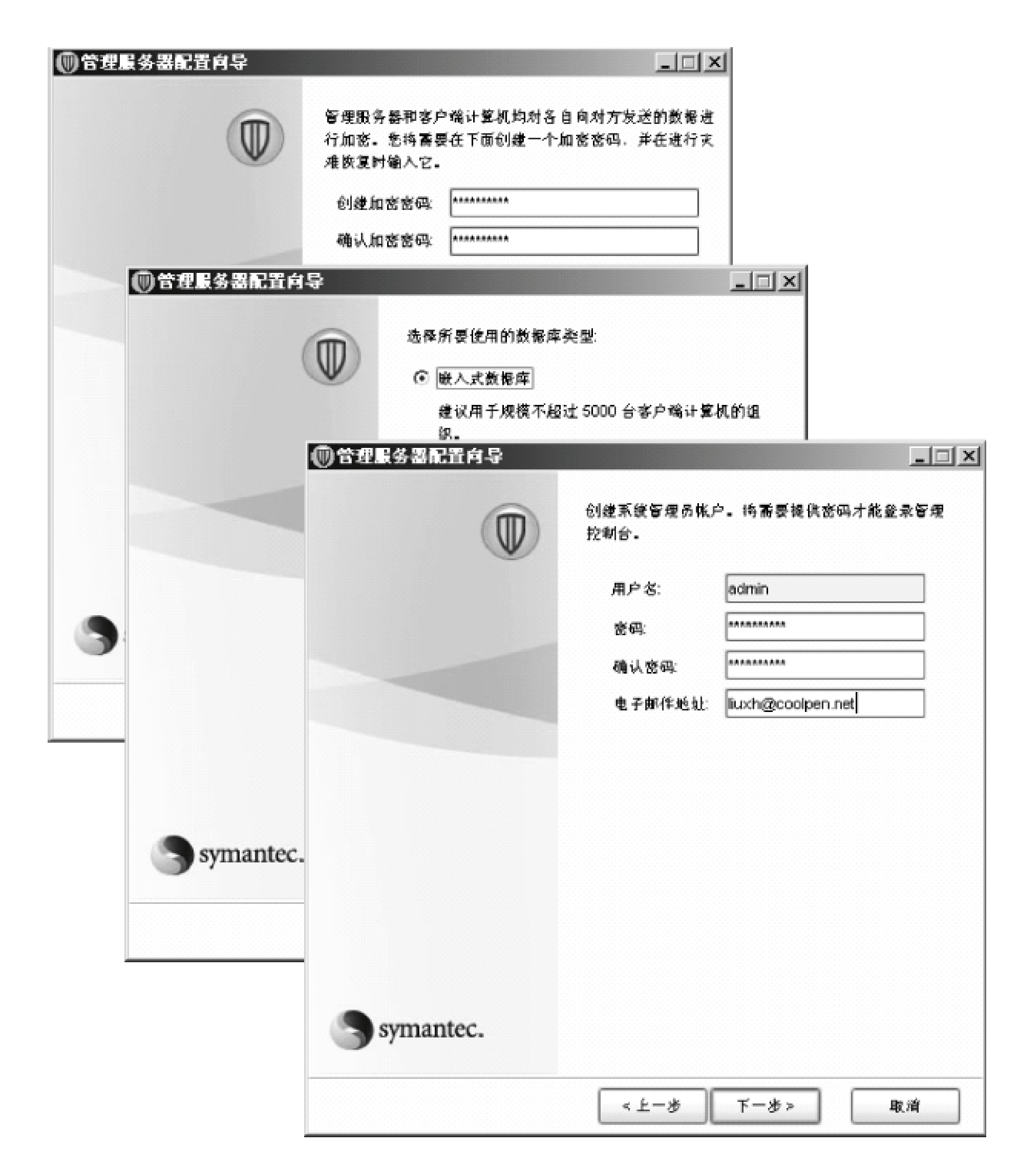


图 5-7　设置密码、数据库类型和管理员账户

5.3.4　迁移和部署向导

迁移和部署向导主要用来帮助管理员完成客户端的部署，或者将客户端从旧版本 Symantec AntiVirus 迁移到 SEP 管理平台。可以在完成“管理服务器配置向导”后立即开

始部署，也可以按照如下方法完成。

（1）依次选择“开始”→“所有程序”→Symantec Endpoint Protection Manager→“迁移和部署向导”选项，显示“欢迎使用迁移和部署向导”对话框。单击“下一步”按钮，选择要进行的操作，选中“部署客户端”单选按钮。单击“下一步”按钮，指定要部署的客户端组。客户端组是对客户端进行统一管理的常用工具，默认情况下，SEP Manager 已经提供了一个名为 Default Group 的组，默认情况下所有采用“拉”方式安装的客户端都将被添加到该组中。选中“指定您要部署客户端的新组名”单选按钮并在文本框中输入组名，则通过此向导部署的客户端将自动加入该组，如图 5-8 所示。



图 5-8 选择要进行的操作和指定组名

（2）单击“下一步”按钮，开始定制该客户端安装包中提供的保护功能，通常保持默认即可。单击“下一步”按钮，显示如图 5-9 所示对话框，定制安装包的类型及安装方式。使用默认配置创建的安装程序将适用于 32 位客户端，文件格式为 EXE，且在无人参与情况下完成安装。单击“浏览”按钮，可以设置存储安装程序的目标文件夹，注意此处的文件夹路径必须全部用英文表示，即必须遵循表 5-2 所示的国际化准则。

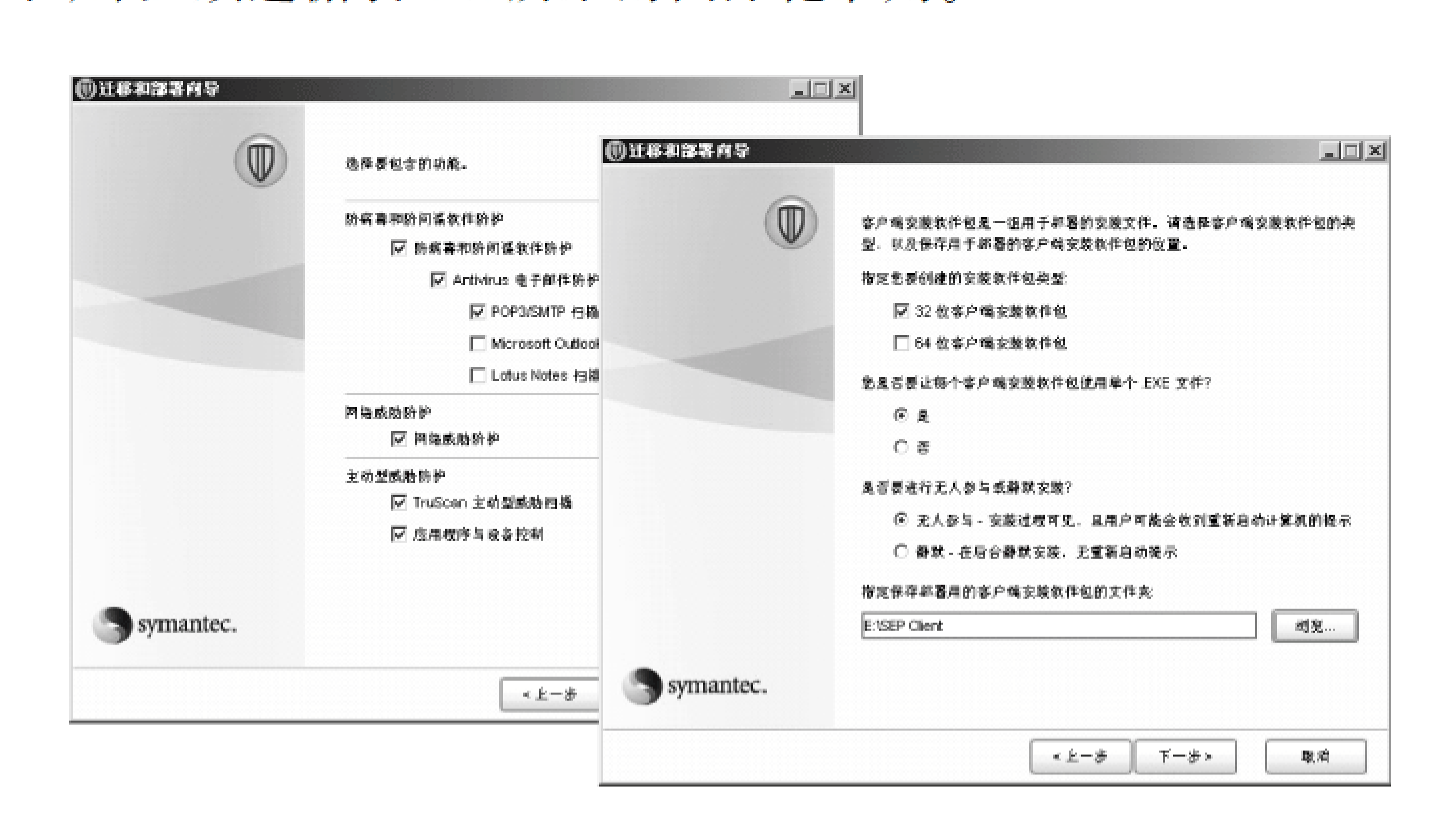


图 5-9 设置安装包相关选项

表 5-2　国际化命名准则

组　　件	命 名 准 则
计算机名、域名及工作组名	支持非英文字符时的限制如下： ① 对于那些使用双字节字符集或 hi-ASCII 字符集的名称，网络审核功能可能无法正常工作 ② 在 SEP Manager 控制台或 SEP 客户端用户界面上，双字节字符集名称或 hi-ASCII 字符集名称可能无法正常显示 ③ 较长的双字节或 hi-ASCII 字符集主机名不能长于 NetBIOS 允许的长度。如果主机名长于 NetBIOS 允许的长度，则 SEP Manager 控制台上不显示“主页”、“监视器”和“报告”页面 ④ 以双字节或 hi-ASCII 字符名称命名的客户端计算机用作组更新提供程序时无法工作
在下列情况下只使用英文字符	① 将客户端软件包部署到远程计算机 ② 在 SEP Manager 的服务器配置向导页中定义服务器数据文件夹 ③ 定义 SEP Manager 的安装路径 ④ 在将客户端部署到远程计算机时定义凭据 ⑤ 定义组名称。可以为名称中包含非英语字符的那些组创建客户端软件包。但是，当组名中包含非英语字符时，可能无法使用“推式部署向导”部署客户端软件包 ⑥ 将非英语字符推送至客户端计算机。在服务器端生成的某些非英语字符在客户端用户界面上可能无法正确显示。例如，双字节字符集位置名称在以非双字节字符集命名的客户端计算机上无法正确显示
客户端计算机上的“用户信息”对话框	安装完导出的软件包之后，在客户端计算机上的“用户信息”对话框中提供反馈时，不要使用双字节字符或 hi-ASCII 字符
启用 SQL Server 中的 I18n 支持	使用 SQL Server 数据库的双字节、hi-ASCII 或混合语言环境需要启用批处理模式。 管理员可以在 SQL Server 中启用 I18n 支持

（3）单击“下一步”按钮，开始制作安装包，完成后会提示是否立即部署到远程客户端，如果选中“是”单选按钮，则完成向导后将立即开始在远程计算机上安装 SEP 客户端。单击“完成”按钮，关闭“迁移和部署向导”即可，默认情况下将自动启动“Symantec Endpoint Protection Manager 控制台”，显示如图 5-10 所示的登录窗口。

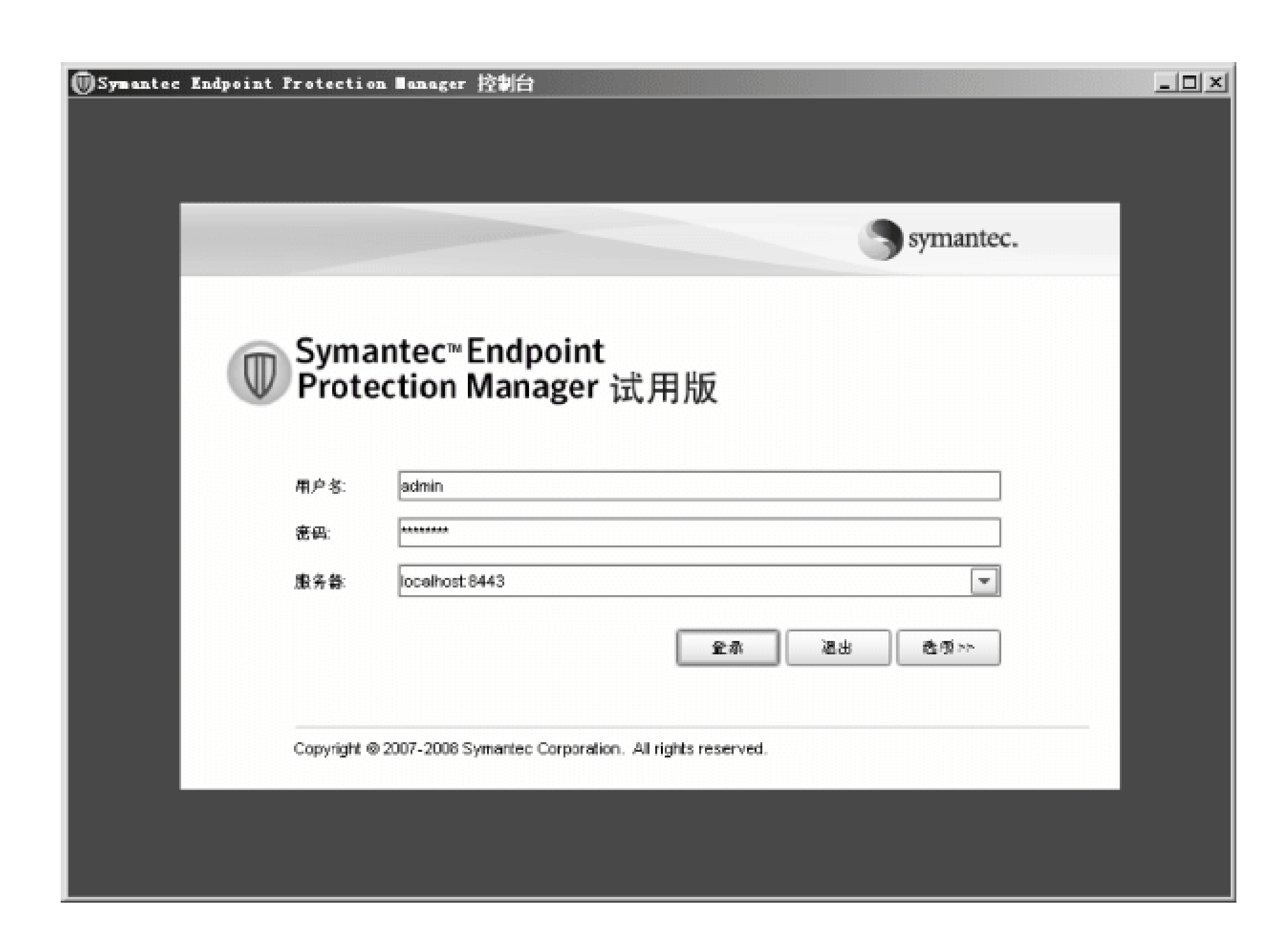


图 5-10　登录 SEP Manager 控制台

5.3.5 知识链接：SEP

1. SEP

SEP(Symantec Endpoint Protection,Symantec 端点保护)是 Symantec 公司推出的新一代企业版网络安全防护产品，它将 Symantec AntiVirus 与高级威胁防御功能相结合，可以为笔记本电脑、台式机和服务器提供安全防护能力。新一代 Symantec 代安全防护产品主要包括 SEP 和 SNAC(Symantec Network Access Control,Symantec 端点网络访问控制)两种。其中，SEP 产品提供了功能强大的 SEP Manager，可以帮助管理员快速完成网络安全的统一部署和管理。

SEP 可保护端点计算设备不受病毒威胁和风险侵袭，并为端点计算机提供 3 层防护，分别是网络威胁防护、主动型威胁防护以及防病毒和防间谍软件防护，如图 5-11 所示。网络威胁防护通过使用规则和特征，可禁止威胁访问被保护计算机。主动型威胁防护可根据威胁的行为，标识并降低威胁。防病毒和防间谍软件防护使用 Symantec 创建的特征，识别并削弱尝试访问或已访问被保护计算机的威胁。

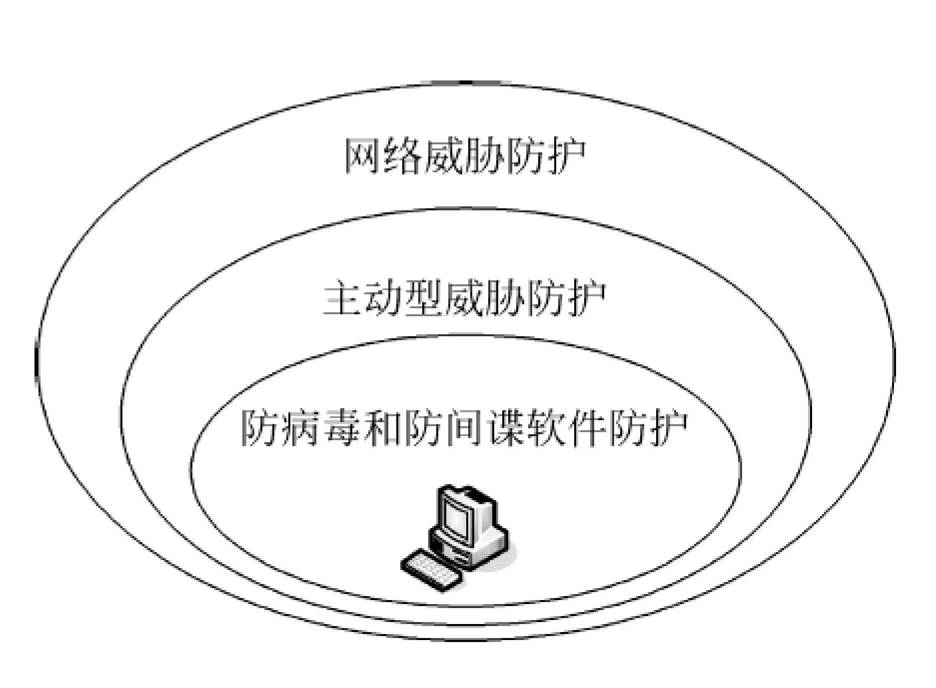


图 5-11 SEP 的 3 层防护示意图

(1) 网络威胁防护

网络威胁防护包括防火墙和入侵防护软件，可保护端点计算设备。防火墙支持为特定端口和特定应用程序写入的规则，并对所有网络通信使用状态检查。因此，对于由客户端发起的所有网络通信，只需要创建出站规则即可支持该通信。状态检查会自动允许响应出站通信的返回通信。防火墙完全支持 TCP、UDP、ICMP 和所有 IP 协议(如 ICMP 和 RSVP)。防火墙还支持以太网和令牌环协议，且可以禁止协议驱动程序，如 VMware 和 WinPcap。防火墙可自动识别合法的 DNS、DHCP 和 WINS 通信，因此可以选中复选框以允许此通信，而不写入规则。

入侵防护引擎支持检查端口扫描和拒绝服务攻击，并可阻挡缓冲区溢出攻击。此引擎也支持自动禁止来自受感染计算机的恶意通信。入侵检测引擎支持深度数据包检查、正则表达式，并且可让用户创建使用类似 Snort 格式的自定义特征。

(2) 主动型威胁防护

主动型威胁防护可根据计算机上进程的行为识别威胁，例如，蠕虫、病毒、特洛伊木马，以及记录键盘记录程序。TruScan 主动型威胁扫描根据这些威胁的行为和特性(而不是根据传统的安全特征)来识别它们。主动型威胁扫描会针对数百种的检测模块分析威胁的行为，以确定活动的进程是安全的还是具有恶意的。此项技术可以在不使用传统特征码或补丁程序的情况下，通过威胁的行为立即检测和降低未知的威胁。

在支持的 32 位操作系统上，主动型威胁防护还可控制对硬件设备、文件和注册表的读取、写入和执行访问。用户可以通过类 ID 禁用外围设备(例如 USB、蓝牙、红外线、FireWire、串口、并口、SCSI 和 PCMCIA)。

(3) 防病毒和防间谍软件威胁防护

防病毒和防间谍软件威胁防护通过扫描引导扇区、内存与文件，看其中是否有病毒、间

谍软件和安全风险，防止计算机受感染。防病毒和防间谍软件威胁防护使用病毒和安全风险特征，可在病毒定义文件中找到这些特征。此防护通过在不造成计算机不稳定的情况下，在安全风险安装前先予以禁止，也可保护计算机。

防病毒和防间谍威胁防护包括自动防护，可检测尝试访问内存或自行安装的病毒和安全风险。自动防护也会扫描安全风险，如广告软件和间谍软件。当它发现安全风险时，会将受感染文件隔离，或者消除和弥补安全风险的负面影响。也可以在自动防护中禁用安全风险扫描。自动防护可修复复杂的风险，例如，隐藏用户模式风险（Rootkit）。自动防护还可修复难以删除或者会重新自我安装的永久性安全风险。

防病毒和防间谍软件威胁防护也包括自动防护，通过监控所有 POP3 和 SMTP 通信，扫描 Internet 电子邮件程序。用户可以配置防病毒和防间谍软件威胁防护，使其扫描传入消息是否有威胁和安全风险，以及扫描传出消息是否进行已知启发式扫描。扫描传出电子邮件有助于阻止威胁（如蠕虫）的传播，它们可以使用电子邮件客户端在网络上进行复制。

2．SEP Manager

SEP Manager 包含 Web 的应用程序，因此安装之前必须先安装 IIS 组件。SEP Manager 包括一个嵌入式数据库，以及 SEP Manager 控制台。用户既可以自动安装嵌入式数据库，也可以将数据库指定到 Microsoft SQL Server 2000/2005 实例中。如果支持业务的网络属于小型网络，且位于一个地理位置，那么只需要安装一个 SEP Manager。如果网络分散在不同地点，则可能需要安装额外的 SEP Manager，以用于负载平衡和带宽分配。如果网络规模庞大，则需要安装带有附加数据库的额外 SEP Manager 站点，并将其配置为通过复制共享数据。

（1）SEP Manager 的工作方式

用户可以根据需要将客户端安装为受管客户端或非受管客户端。受管网络可充分利用网络的功能。网络上的每个客户端和服务器都可通过运行 SEP Manager 的一台计算机进行监控、配置和更新。用户也可以从 SEP Manager 控制台安装和升级 SEP 与 SNAC 客户端。

在非受管网络中，必须单独管理每台计算机，或将管理职责转交给该计算机的主要用户。对于信息技术资源有限或匮乏的小型网络，应采用这种方法，相关职责如下。

① 更新病毒及安全风险定义。

② 配置防病毒及防火墙设置。

③ 定期升级或迁移客户端软件。

注意：如果要允许用户更改客户端设置，建议最好将客户端安装于受管环境中。

在受管网络中，用户可以将客户端计算机分成组。使用这些组，可将需要相似访问级别和配置设置的客户端放在同一组。用户可以选择在组中指定不同的位置设置。如果客户端是从不同的位置访问网络，则可应用不同的策略。还可以从 SEP Manager 控制台创建、查看和配置组。

（2）SEP Manager 的功能

使用 SEP Manager 可执行下列操作。

① 建立和强制实施安全策略。

② 防止受到病毒、混合型威胁以及安全风险（如广告软件和间谍软件）的侵害。

③ 利用集成的管理控制台来管理病毒防护的部署、配置、更新和报告。

④ 防止用户访问计算机的硬件设备,例如USB驱动器。

⑤ 利用集成的管理控制台来管理病毒防护、防火墙防护和入侵防护的部署、配置、更新和报告。

⑥ 管理客户端及其位置。

⑦ 标识过期的客户端,迅速应对病毒爆发,并部署更新的病毒定义。

⑧ 创建和维护详细描述网络中发生的重要事件的报告。

⑨ 为连接到网络的所有用户提供针对安全威胁的高级别的防护和集成响应。此防护覆盖始终保持网络连接的远程办公人员和间歇连接到网络的移动用户。

⑩ 获得分布在网络上的所有工作站的多个安全组件的合并视图。

⑪ 对所有安全组件执行可定制的、集成的安装并同时设置策略。

⑫ 查看历史记录和日志数据。

5.4 安装SEP客户端

SEP客户端可分为非受管客户端和受管理客户端,其中受管理客户端可以通过SEP Manager远程部署等方式安装,也可以在客户端上使用管理服务器创建的安装包安装,安装完成后将自动添加到指定组中,并接受服务器的统一管理。而非受管客户端则可以通过安装光盘完成,虽然同样可以被添加到服务器控制台中,但不接受服务器的管理。需要注意的是,SEP在安装过程中需要至少700MB的硬盘空间,如果空间不足,将导致安装失败。

5.4.1 安装受管理客户端

用户可以通过多种方式安装接受统一管理的SEP客户端,常用的有如下两种。

1. 迁移和部署向导的"推"式安装

在创建客户端安装包过程中可以同时将定制完成的安装程序部署到客户端,也可以选择创建完成后保存到服务器上,需要部署时再通过"迁移和部署向导"完成。需要注意的是,Windows Vista系统中的用户访问控制(UAC)功能禁止本地管理账户远程访问远程管理共享,如C$和ADMIN$,使用该方式部署时应将其关闭。接下来,介绍一下如何使用现有安装包部署受管理客户端。

(1) 启动"迁移和部署向导",连续单击"下一步"按钮,直至显示如图5-12所示对话框,选中"选择现有客户端安装软件包以进行部署"单选按钮。



图5-12 选择部署方式

(2) 单击"完成"按钮,显示"推式部署向导"对话框,单击"浏览"按钮,选择已经创建完成的安装程序所在目录,在"指定并行部署数量上限"文本框中输入相应的值(以管理服务器性能而定),默认为10个。单击"下一步"按钮,在"可用计算机"列表中,展开Microsoft Windows Network→"工作组名或域名"并选

择希望添加作为客户端的计算机，如图 5-13 所示。

图 5-13　选择安装包路径和要部署的计算机

提示：如果本地计算机上的“Computer Browser 服务”没有启动，则无法展开 Microsoft Windows Network 下的计算机列表。如果“Windows 防火墙”的“例外”列表中没有对“文件和打印机共享”启用例外，则该服务将无法启动。

注意：第一次部署客户端时必须确保已经包含本地计算机，即必须先为本地计算机安装 SEP 客户端，否则 SEP Manager 控制台中将无法发现已部署的 SEP 客户端。

(3) 单击“添加”按钮，显示如图 5-14 所示的“远程客户端验证”对话框，在“用户名”和“密码”文本框中输入远程登录目标计算机时使用的账户信息，单击“确定”按钮即可将其添加到“要部署到的计算机”列表中。重复操作可以同时添加多个客户端。

提示：如果远程计算机上没有开启网络共享，或者启用了 Windows 防火墙，则此处可能无法正常添加计算机，会出现“无任何网络提供程序接受指定的网络路径”类似信息。此时只需开启防火墙和系统共享(尤其是系统默认共享)即可。如果目标计算机是 Windows Server 2008 Server Core 系统，则可以执行如下命令将共享添加到 Windows 防火墙允许的应用程序中：

```
netsh firewall set service fileandprint enable
```

(4) 添加完所有需要部署的客户端后，单击“完成”按钮，即可开始安装，显示如图 5-15 所示的“远程客户端安装状态”对话框。单击“关闭”按钮即可关闭对话框，提示是否查看部署日志。如果并发部署的客户端较多，则可能由于服务器性能导致部分客户端无法正常完成，此时即可通过部署日志确定完成情况。

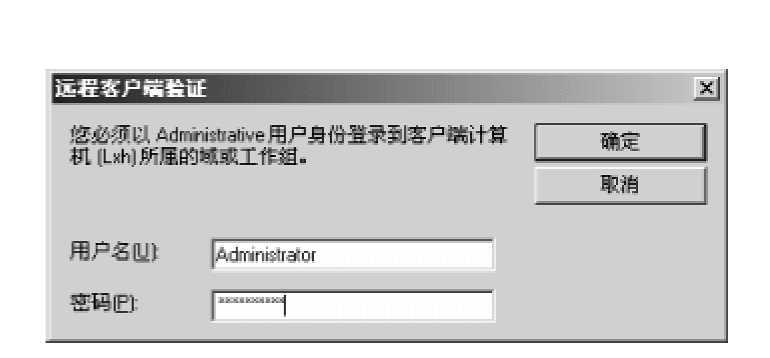


图 5-14　“远程客户端验证”对话框

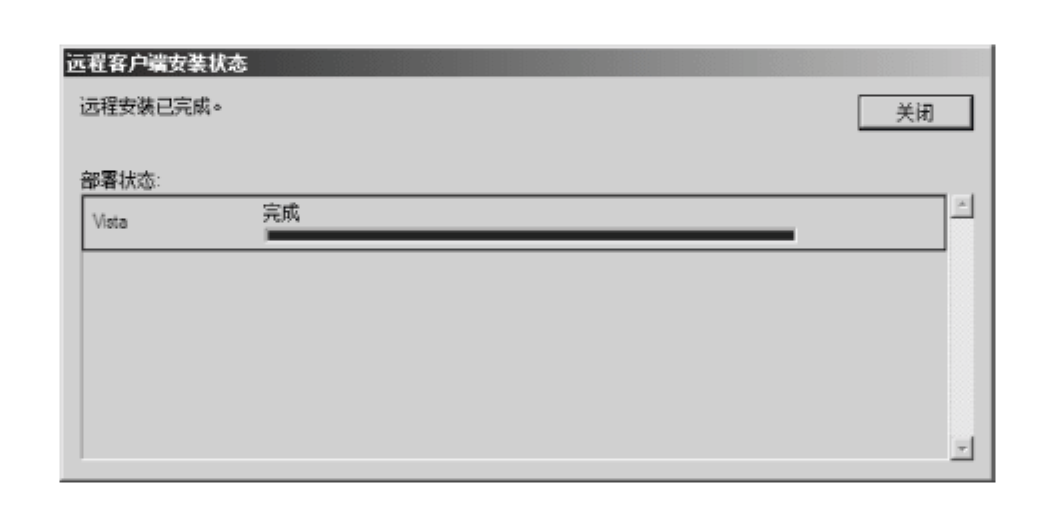


图 5-15　“远程客户端安装状态”对话框

至此，管理服务器上的远程部署工作已完成，客户端将开始自动安装，安装完成后将提示用户是否立即重新启动计算机和更新病毒库，按照要求操作即可。

2. 使用“查找非受管计算机”部署

管理员可使用 SEP Manager 控制台中的“查找非受管计算机”部署客户端软件。使用此实用程序，可以扫描没有运行客户端软件的客户端计算机，然后在这些计算机上安装客户端软件。

(1) 登录到“Symantec Endpoint Protection Manager 控制台”，单击左侧“客户端”标签，在“任务”列表中单击“查找非受管计算机”链接，显示如图 5-16 所示的“查找非受管计算机”对话框。在“搜索依据”选项区域内选中“IP 地址范围”单选按钮，并设置起止 IP 地址。在“登录证书”选项区域，输入登录客户端计算机的凭证及所在工作组或域。单击“立即搜索”按钮即可开始搜索，搜索结果将显示在“非受管计算机”和“未知的计算机”列表中，默认显示“非受管计算机”。

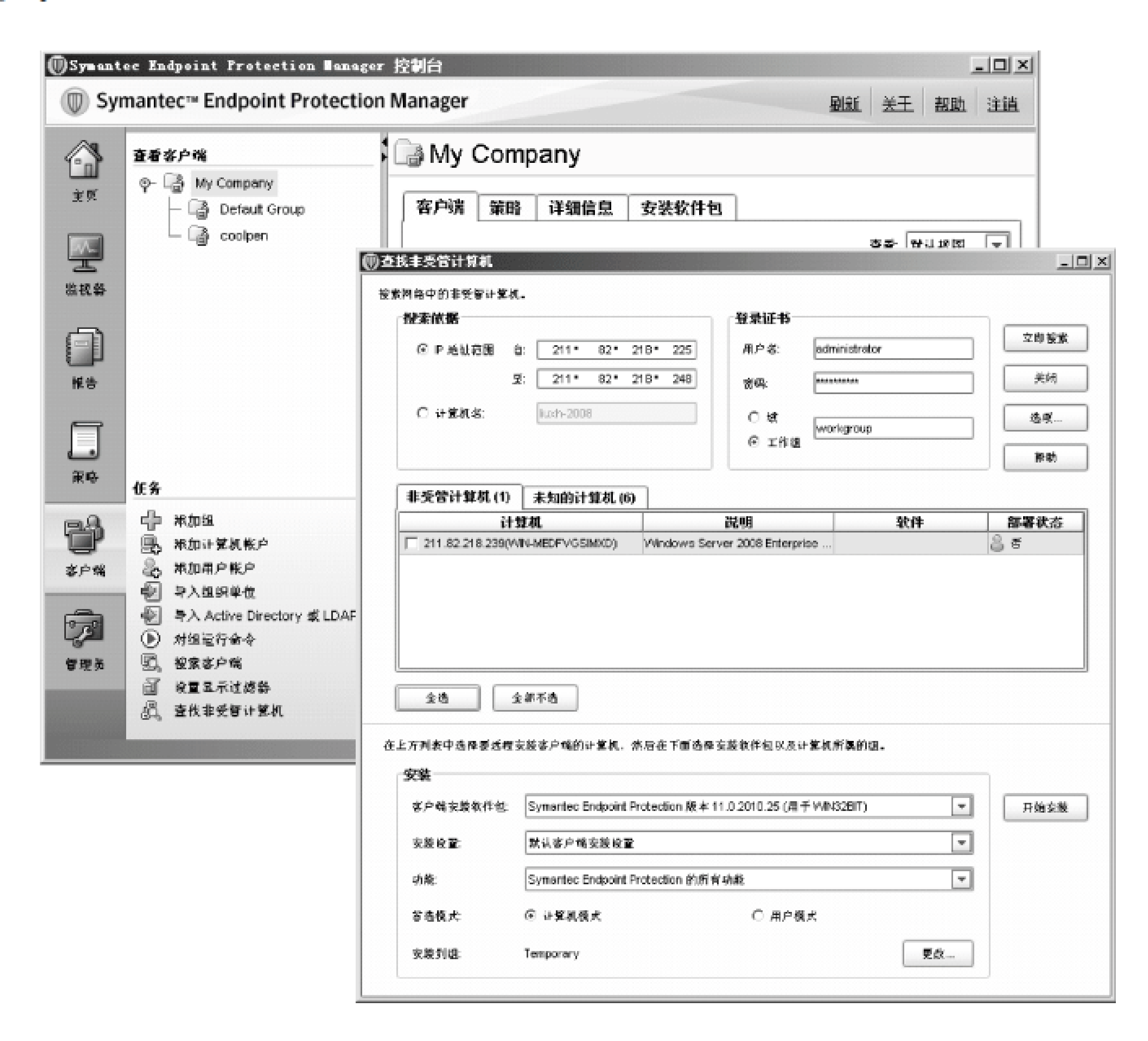


图 5-16 “查找非受管计算机”对话框

提示：“非受管计算机”列表中显示的是安装非受管客户端的计算机，或者曾经安装过客户端但现在已经卸载的；“未知的计算机”列表中显示的是当前网络中所有没有部署 SEP 客户端的计算机。

(2) 选中希望部署的对象，并在“安装”选项区域设置相应的安装选项。在“客户端安装软件包”下拉列表框中选择适用的安装包类型，包括 32 位和 64 位两种，分别用于不同的系统平台；“安装设置”选项保持系统默认值即可；在“功能”下拉列表框中可以定制客户端的基本功能，选择“Symantec Endpoint Protection 的所有功能”即可。默认情况下，被部署的客户端将自动分配到 Default Group 组中，单击“更改”按钮，可以选择想要添加到的组（如 coolpen）。

(3) 单击“开始安装”按钮即可开始将 SEP 客户端“推”安装到目标计算机上。完成后显

示如图 5-17 所示结果,“部署状态”显示为“成功”即表明客户端安装成功。“推”安装过程中,客户端不会提示任何信息,在安装完成后,才会提示用户升级病毒库。

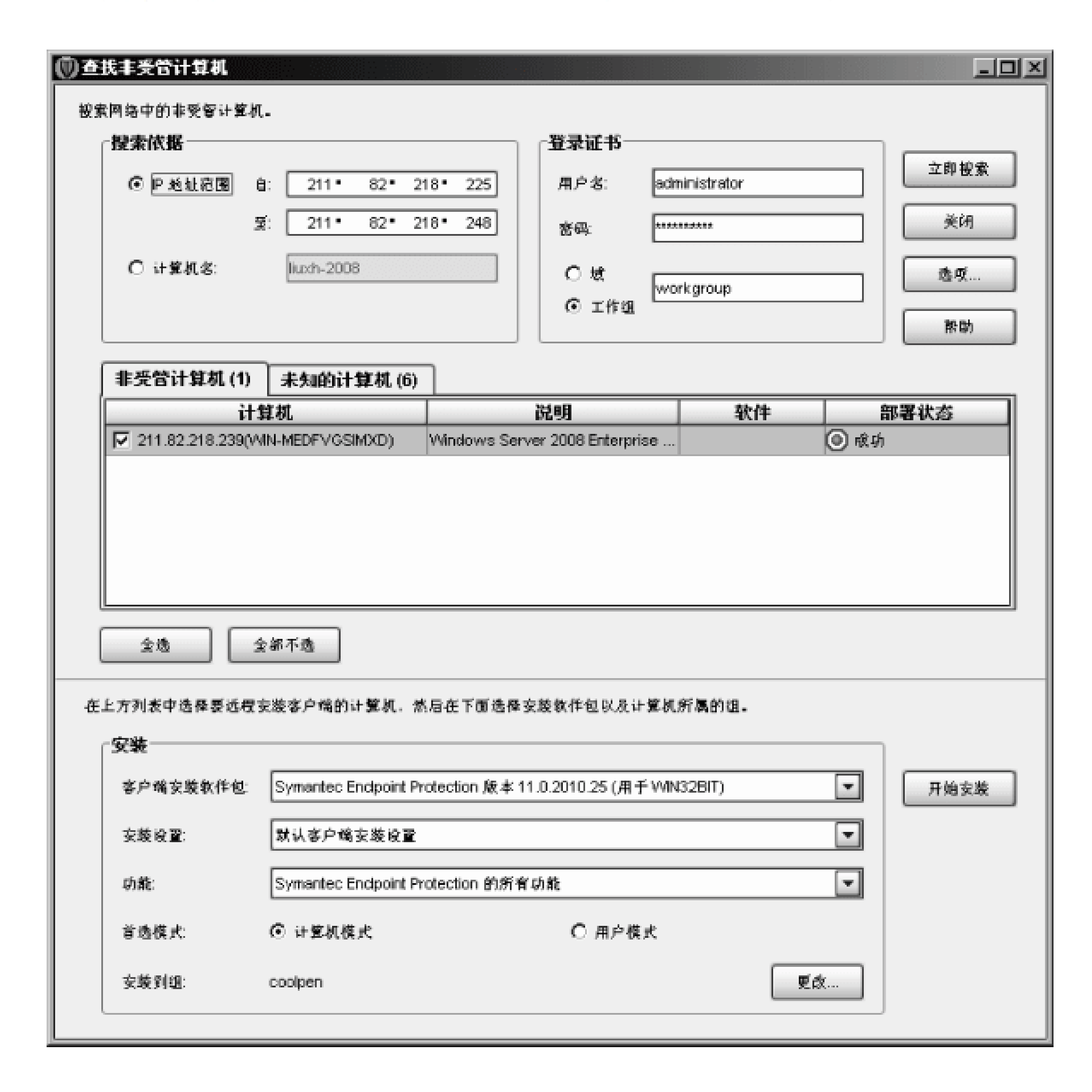


图 5-17　部署成功

5.4.2　部署非受管客户端

SEP 非受管客户端的部署通常是借助安装光盘完成的,安装过程并不复杂,而对于 Windows Server 2008 Server Core 系统而言,由于系统仅提供了命令行界面,必须借助相关命令完成客户端的部署,对于不熟悉命令操作的管理员而言,可能会有点难度。

1. 部署 Windows Vista 非受管客户端

以 Windows Vista 系统为例,通过安装光盘部署 SEP 非受管客户端的操作步骤如下。

(1) 插入 SEP 安装光盘,光盘自动运行显示如图 5-18 所示的“Symantec Endpoint Protection 安装程序”对话框。如果未能自动运行,可以在“资源管理器”中运行光盘根目录下的 setup.exe 文件启动安装程序。

(2) 单击“安装 Symantec Endpoint Protection”按钮启动 SEP 安装向导,需要接受相关的许可协议,连续单击“下一步”按钮,选中“非受管客户端”单选按钮即可。单击“下一步”按钮,系统默认选中“典型”单选按钮,也可以根据需要选中“自定义”单选按钮,并选择欲安装的安全防护功能,建议系统默认设置,如图 5-19 所示。

(3) 单击“下一步”按钮,显示“准备安装程序”对话框,提示向导已准备好,可以开始安装。单击“安装”按钮即可开始安装,由于 SEP 客户端中集成的功能和组件比较多,可能需要较长的安装时间。安装完成后,显示如图 5-20 所示的“InstallShield 向导完成”对话框。

(4) 单击“完成”按钮,关闭安装向导。默认情况下,将自动启动 LiveUpdate 向导更新病毒库。最后,系统会提示如图 5-21 所示的“重新启动通知”对话框,提示必须重新启动计算机方可使 SEP 的配置生效。

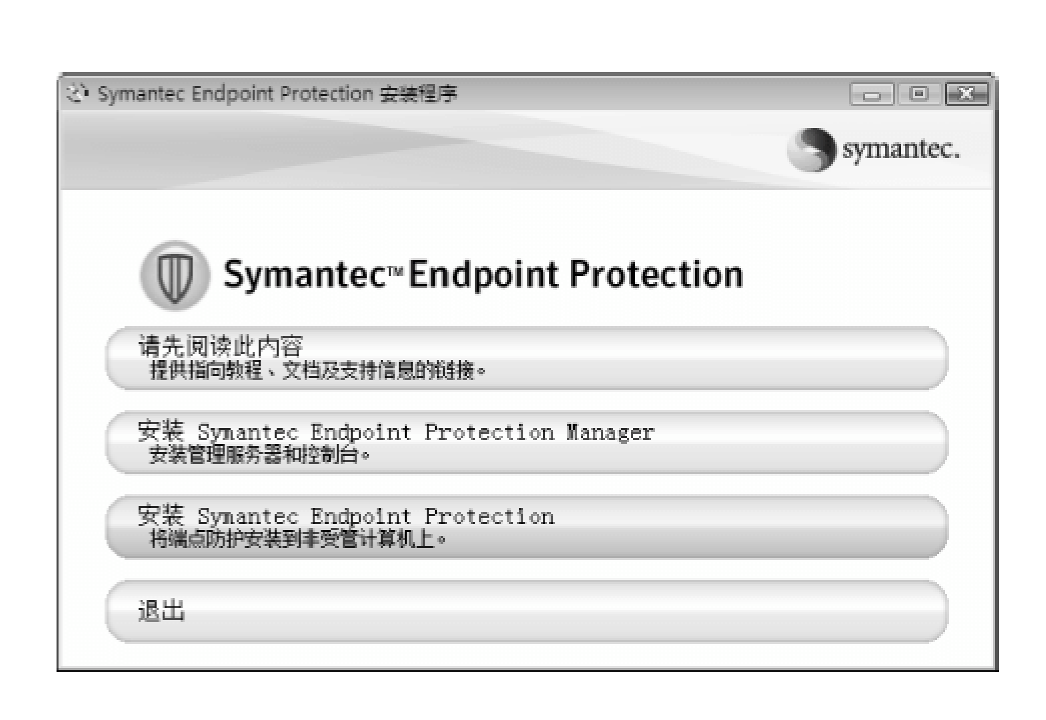


图 5-18 “Symantec Endpoint Protection 安装程序”对话框



图 5-19 设置客户端类型和安装类型



图 5-20 “InstallShield 向导完成”对话框



图 5-21 “重新启动通知”对话框

(5) 重新启动计算机后，即可完成非受管客户端的安装。Windows 2000/XP/2003/2008 系统的安装步骤与此类似，这里不再赘述。

2. 在 64 位 Windows Server 2008 Server Core 上安装非受管 SEP 客户端

(1) 插入 SEP 安装光盘，转到光盘根目录下，并执行如下命令转入安装程序所在目录：

```
cd SEPWIN64\X64
```

(2) 执行如下命令：

```
vcredist_x64.exe
```

(3) 转回安装光盘的根目录，输入 setup.exe 并按 Enter 键，即可启动安装向导，借助该向导即可顺利完成 64 位 SEP 客户端的部署。

提示：如果是 32 位 Windows Server 2008 Server Core 系统的计算机，则直接在命令提示符窗口中，转入安装光盘根目录下，执行 setup.exe 文件即可启动安装向导。

5.5　升级病毒库

杀毒软件是根据提取的病毒特征来判断文件是否是病毒程序的，升级病毒库就是不断的更新能够识别的病毒特征，增强杀毒软件与系统应用程序之间的兼容性。通常情况下，非受管客户端将每天自动从 Symantec LiveUpdate 站点升级病毒库。在新一代 Symantec 安全防御系统中，新增了 LiveUpdate 管理服务器，主要为大型网络(超过 5000 个端点)提供客户端病毒库升级管理。

5.5.1　安装 LiveUpdate 管理工具

在安装 LiveUpdate 管理工具之前，必须先在服务器上安装 Java SE 程序，否则无法安装。可以从 Java 官方网站下载，地址为：http://www.java.com。

(1) 运行 SEP 第二张光盘，自动运行后在安装程序界面中单击“安装 LiveUpdate Administrator”按钮，启动 Symantec LiveUpdate Administrator 安装向导，连续单击“下一步”按钮，阅读并接受许可证协议，在“目的地文件夹”对话框中设置 Symantc LiveUpdate Administrator 2.2.1 的安装目录，通常保持默认即可，如图 5-22 所示。

(2) 单击“下一步”按钮，显示如图 5-23 所示的“用户设置”对话框，要求设置默认管理员的用户名、密码和电子邮件地址。该账户用来登录 Symantc LiveUpdate Administrator 控制台和管理 LiveUpdate。

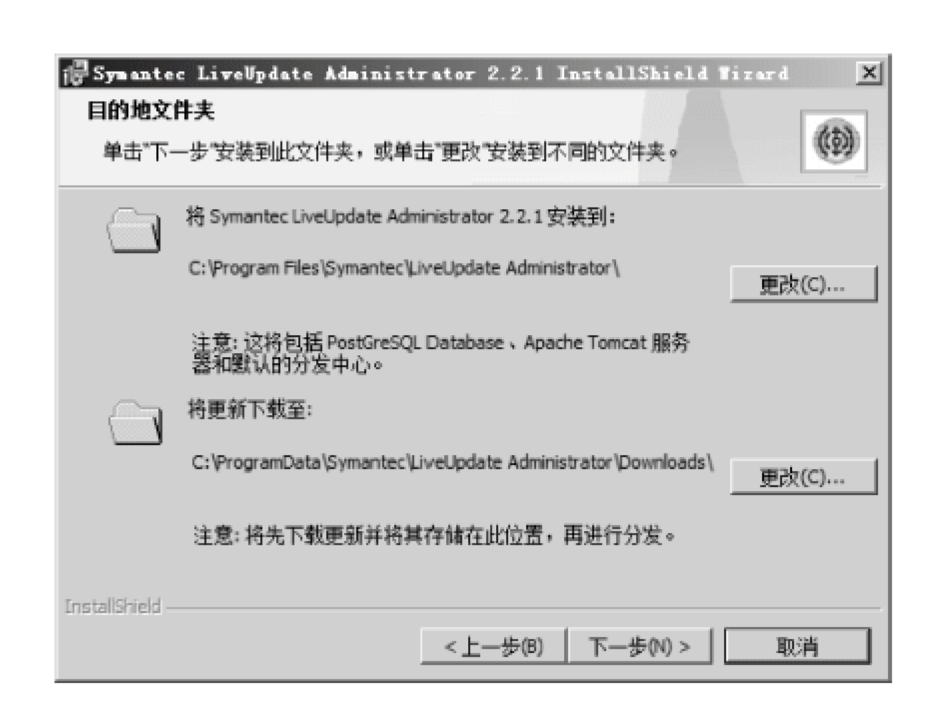


图 5-22　“目的地文件夹”对话框

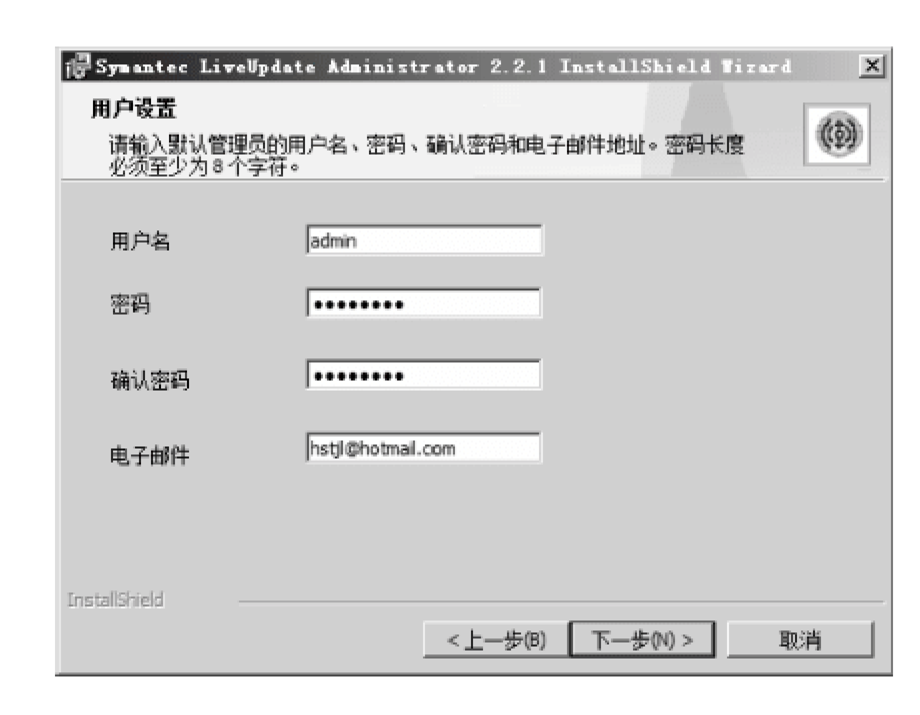


图 5-23　“用户设置”对话框

(3) 连续单击“下一步”按钮，即可开始安装。安装完成后单击“完成”按钮，LiveUpdate 管理工具安装完成。

5.5.2　配置更新

Symantec LiveUpdate Administrator 安装完成以后，需要根据网络中已安装的 Symantec 产品情况，添加需要下载更新的产品。

1. 登录 Symantec LiveUpdate Administrator

(1) 依次选择“开始”→“所有程序”→Symantec LiveUpdate Administrator→LiveUpdate Administrator 2.1 选项，显示如图 5-24 所示的“登录”窗口。分别在“用户名”和“密码”文本框中输入安装时设置的管理员用户名和密码。

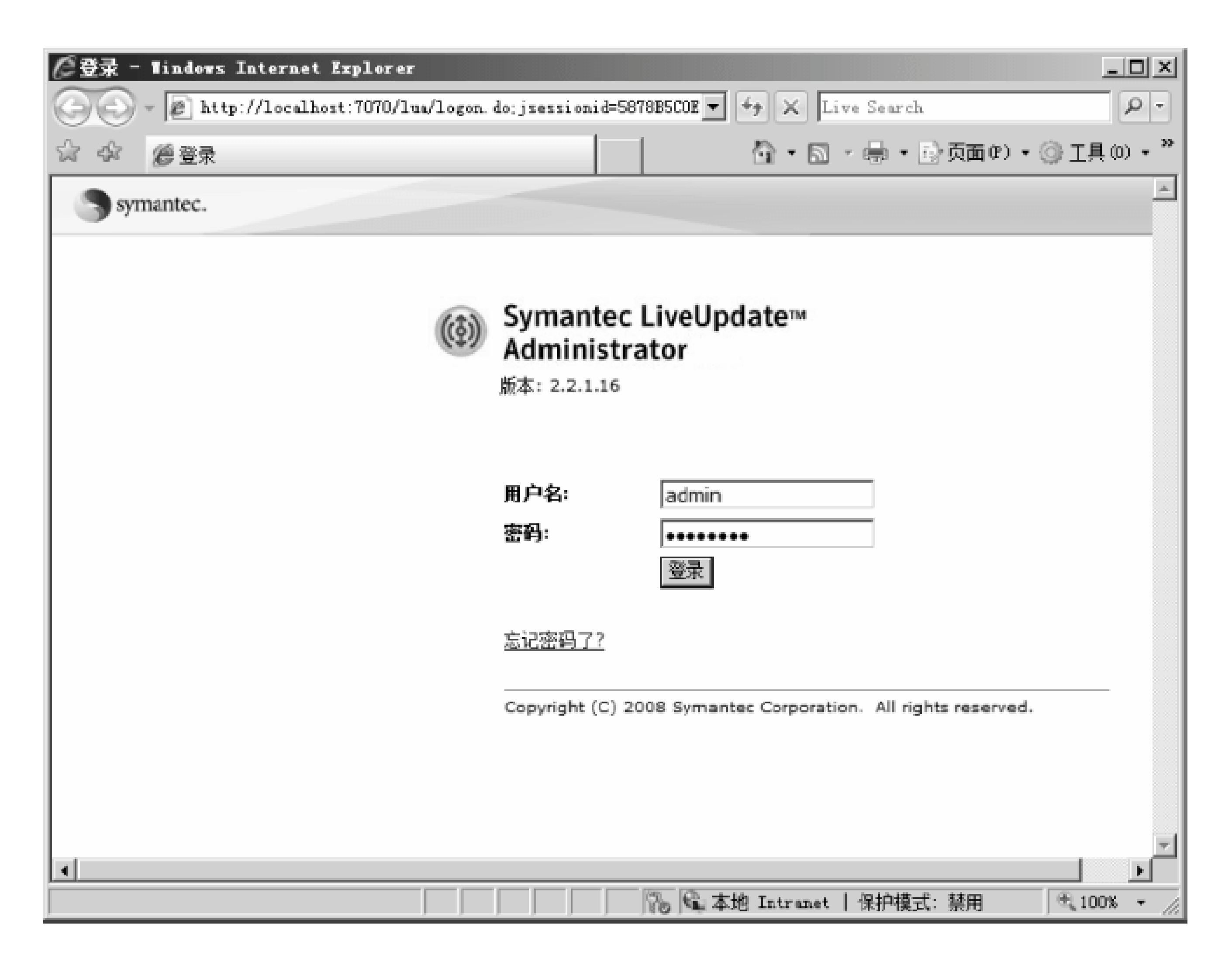


图 5-24 “登录”窗口

(2) 单击“登录”按钮登录，显示如图 5-25 所示的 Symantec LiveUpdate Administrator 窗口。默认显示“主页”，可以查看最近的活动，以及系统信息。



图 5-25 Symantec LiveUpdate Administrator 主页

2. 配置 LiveUpdate

在“配置”窗口中，可以添加要更新的 Symantec 产品、配置下载服务器等。

(1) 在 Symantec LiveUpdate Administrator 窗口中单击“配置”标签，可以添加要更新的产品。单击“添加新产品”按钮，显示“添加到我的 Symantec 产品”窗口。在“产品线”列表中，可以选择要添加的产品，这里选择 Symantec Endpoint Protection。在窗口下方的“所有产品”列表中，可以选择欲添加的产品版本。这里，选择“Symantec Endpoint Protection v11.0 中文版(简体)”，如图 5-26 所示。

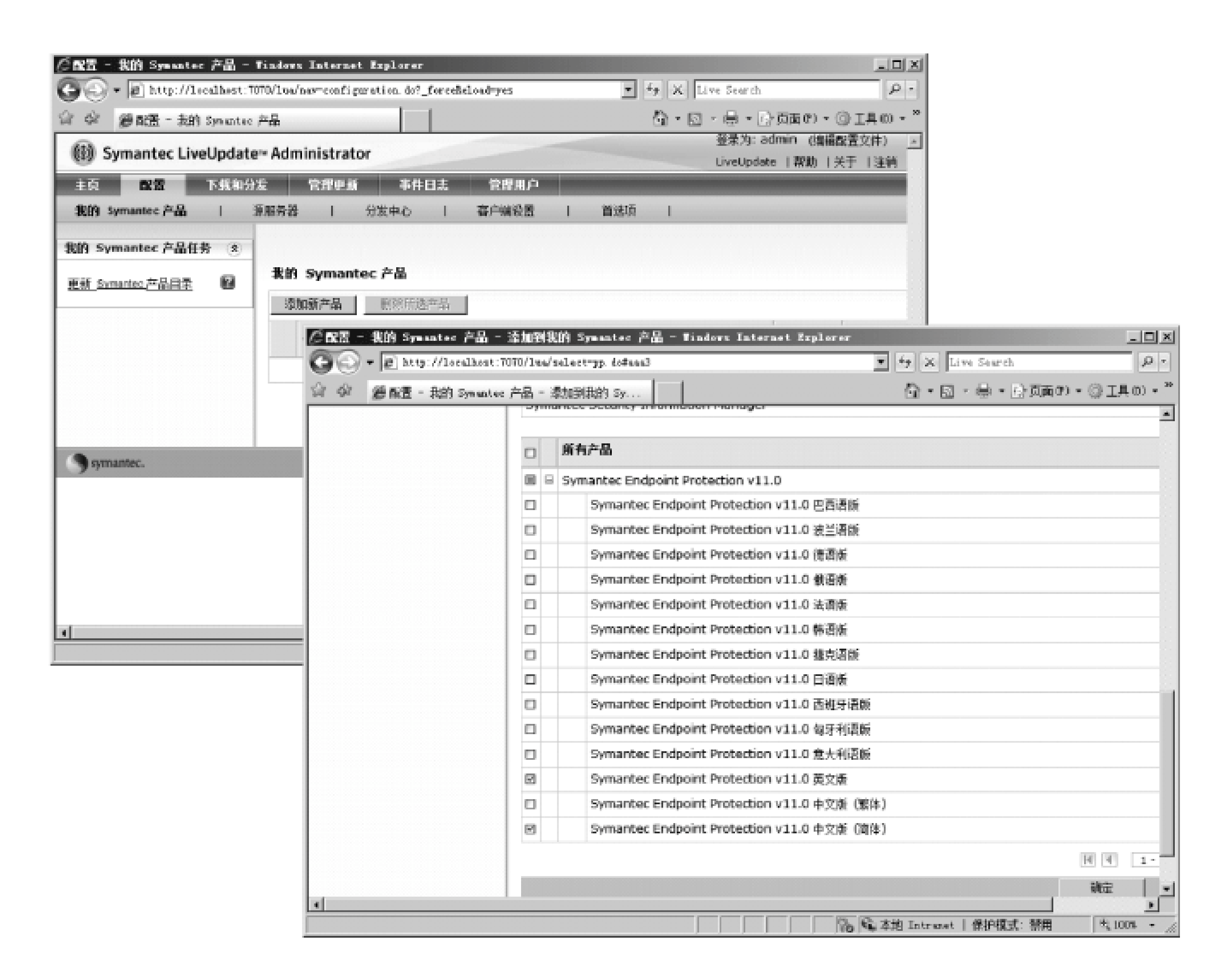


图 5-26　添加 Symantec 产品

（2）单击“确定”按钮，一个 Symantec 产品添加成功，如图 5-27 所示。如果网络中还安装有其他 Symantec 产品，也可以在此处一并添加。

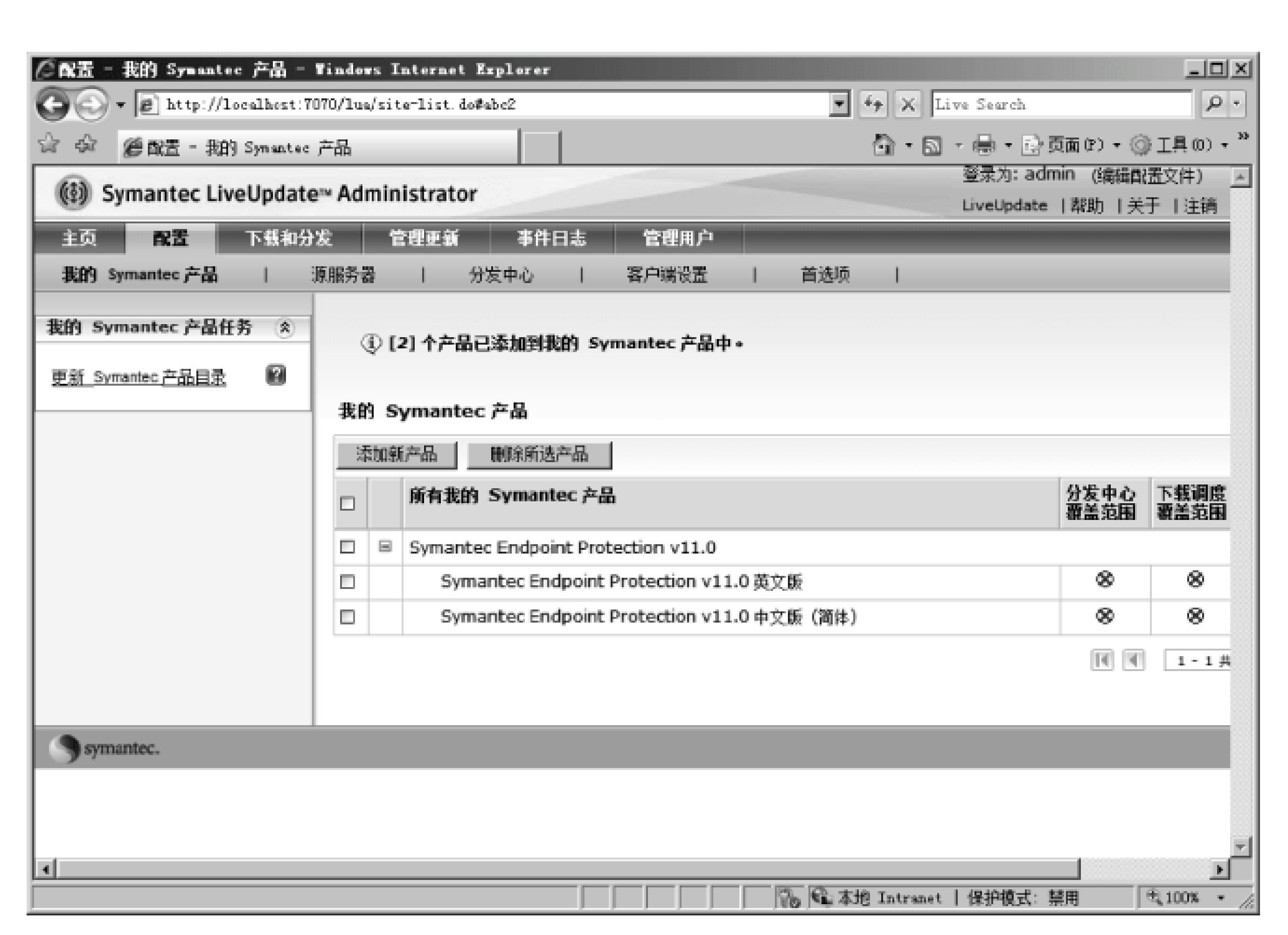


图 5-27　已添加的 Symantec 产品

（3）在“配置”窗口中单击“源服务器”按钮，可以配置 Symantec 产品的更新下载服务器，如图 5-28 所示。默认从 Symantec 的 LiveUpdate 服务器下载。

（4）如果网络中已部分有 LiveUpdate 服务器，则可从本地的 LiveUpdate 服务器上下载，以节省 Internet 带宽。单击“添加”按钮，显示如图 5-29 所示的“新建源服务器”窗口，可以添加本地网络中的 LiveUpdate 地址。

3. 下载和分发

（1）单击“下载和分发”标签，在显示的窗口中单击“添加下载”按钮，显示如图 5-30 所

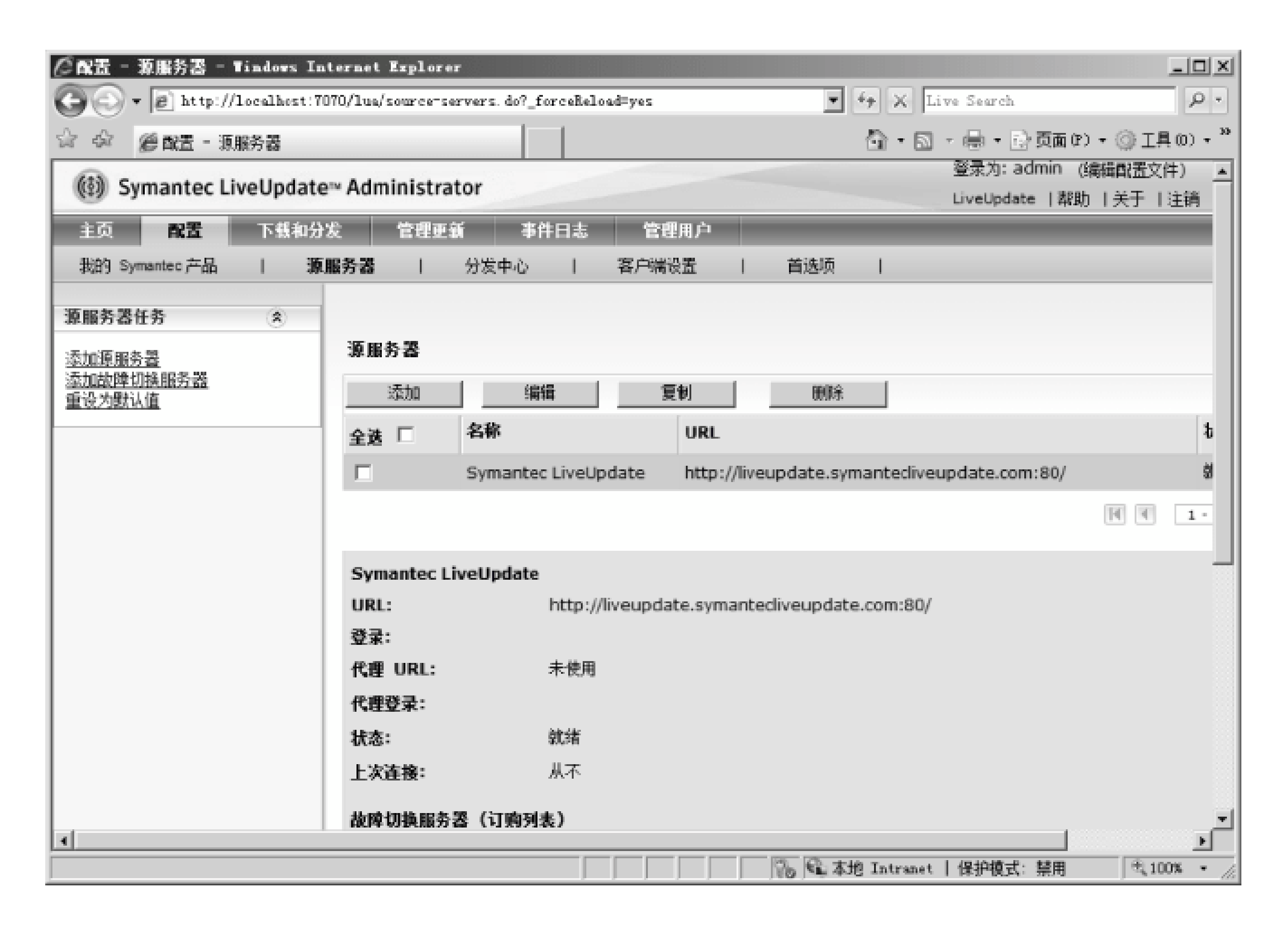


图 5-28 “源服务器”窗口



图 5-29 “新建源服务器”窗口

示的“添加下载调度”窗口，即可开始添加下载调度计划。在“下载调度名称”文本框中输入一个名称，在“状态”下拉列表框中选择“已启用”选项。在“选择产品”选项区域中，需要添加欲下载的产品。单击“添加”按钮，选择要添加的产品即可。

(2) 单击“添加”按钮，将所选择的产品添加到“添加下载调度”窗口中。然后，在“选择产品组件”选项区域中，选择要添加的组件。并在“选择调度”选项区域中，选择计划的执行频率。完成后单击“确定”按钮，一个下载调度添加完成，如图 5-31 所示。

(3) 如果要立即运行下载调度，以下载更新，可选择调度名称，单击“立即运行”按钮，即可开始下载更新，并显示“活动监视器”窗口，显示了当前的下载信息。在列表框中，显示了已下载和正在下载的组件，如图 5-32 所示。

(4) 下载更新完成以后，即可将更新分发到客户端。实施分发之前还需要创建一个分发调度，在“下载和分发”窗口中，单击“添加分发”按钮，显示“添加分发调度”窗口，用来添加

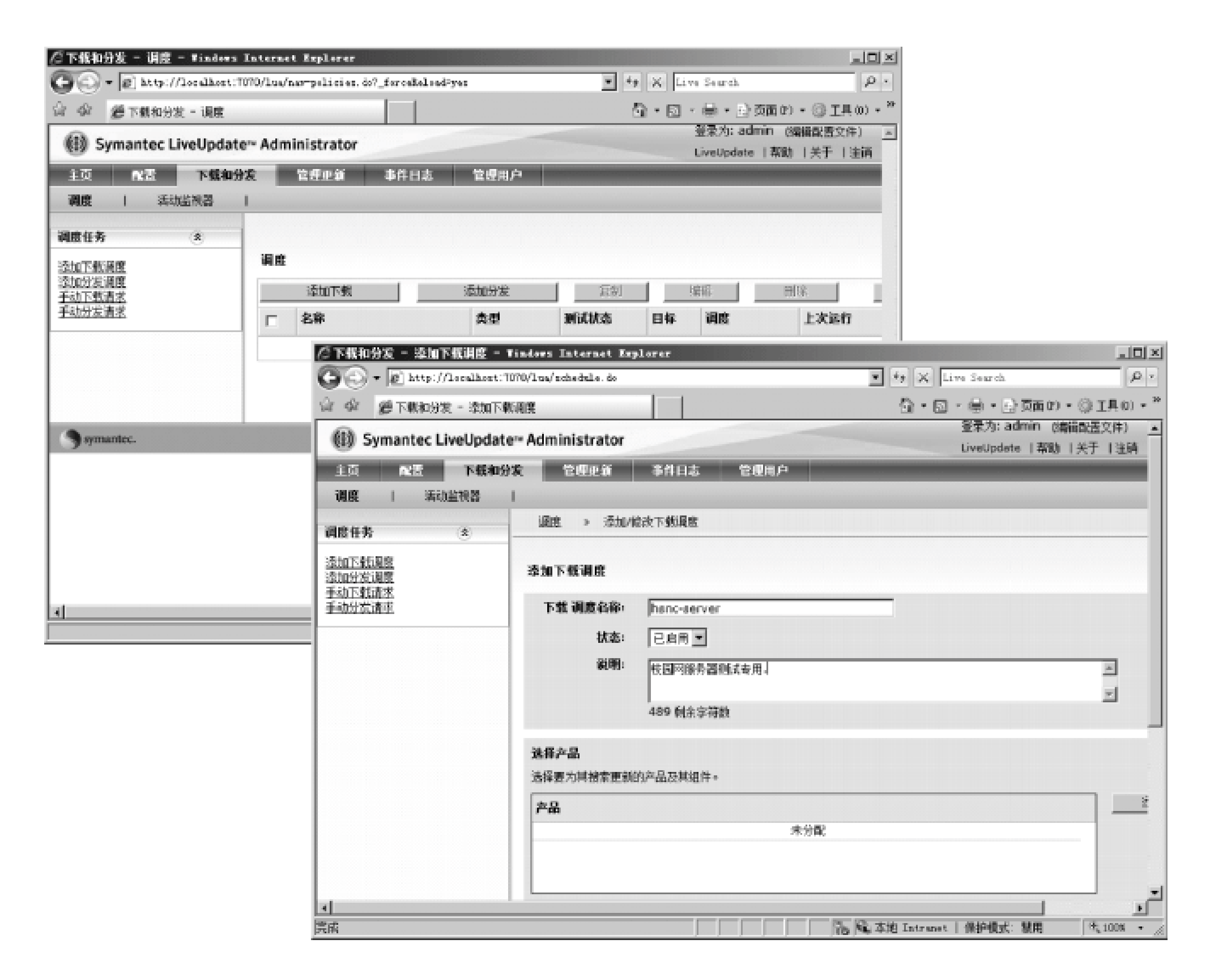


图 5-30　配置下载调度

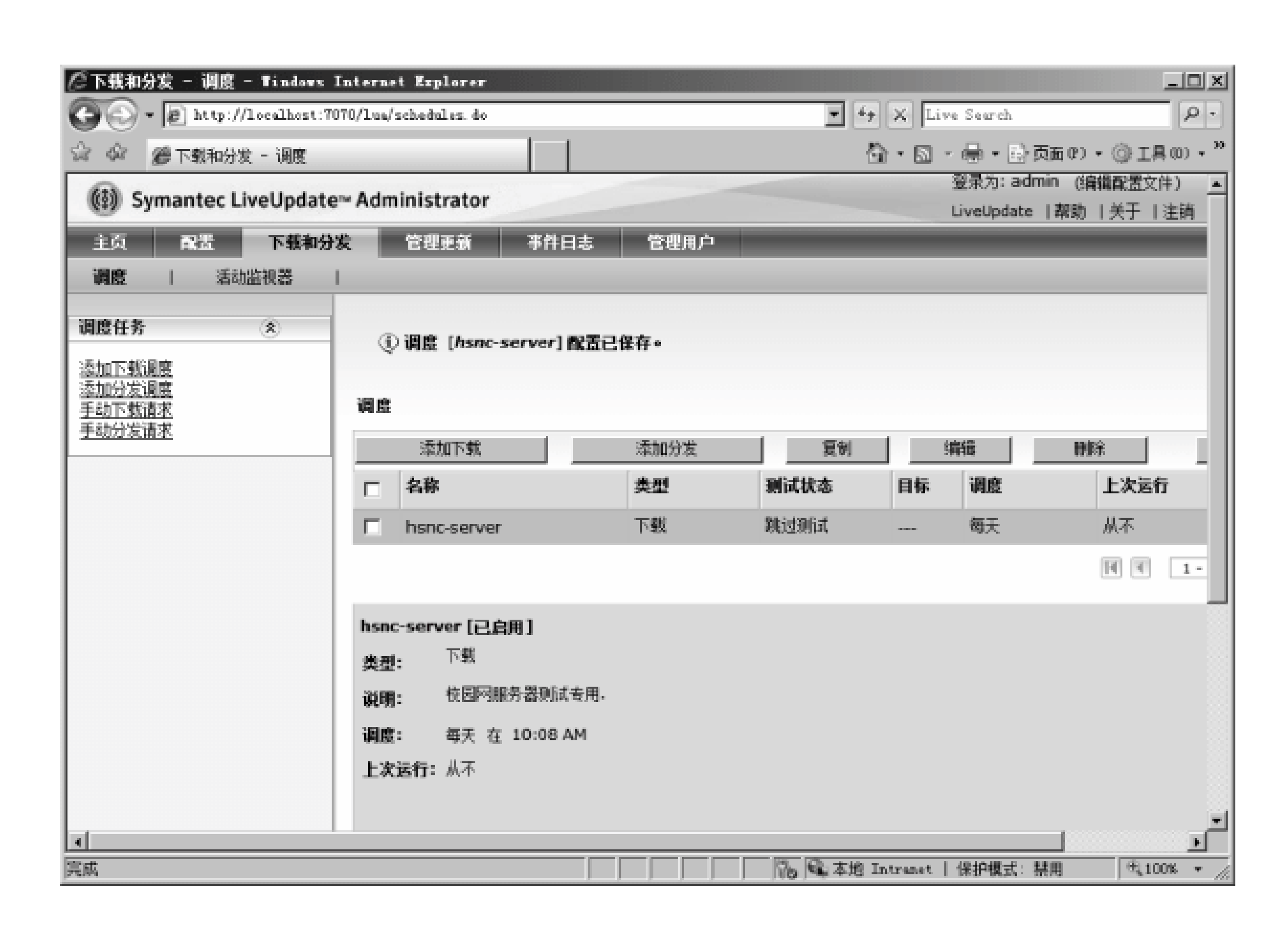


图 5-31　下载调度添加完成

分发调度。在“分发调度名称”文本框中输入一个名称，在“状态”下拉列表框中选择“已启用”选项。在“分发可用于此产品列表的更新”选项区域中，单击“添加”按钮，可以选择要添加的产品；在“选择产品组件”选项区域中，选择要添加的组件；在“选择调度”选项区域中，选择计划的执行频率。完成后单击“确定”按钮，一个下载调度添加完成，如图 5-33 所示。

（5）单击“分发中心”按钮，可以设置分发中心的地址。默认情况下，LiveUpdate 已经创建了两个分发中心，即生产分发中心和测试分发中心，并且均没有添加任何产品。如果要向客户端分发时，必须先向分发中心添加更新，否则不能分发。默认已经创建了产品和测试分发中心。当客户端需要更新时，就需要从该分发中心下载更新程序，如图 5-34 所示。

（6）选中 Default Production Distribution Center 复选框，单击“编辑”按钮，显示“编辑分发中心”窗口。在“产品列表”选项区域中，选择欲添加到分发中心的 Symantec 产品，如

图 5-32　正在下载更新



图 5-33　添加分发调度



图 5-34　“分发中心”窗口

图 5-35 所示。单击“确定”按钮,返回“编辑分发中心”窗口,产品添加完成。单击“确定”按钮保存即可。此时,就可以向客户端分发更新了。

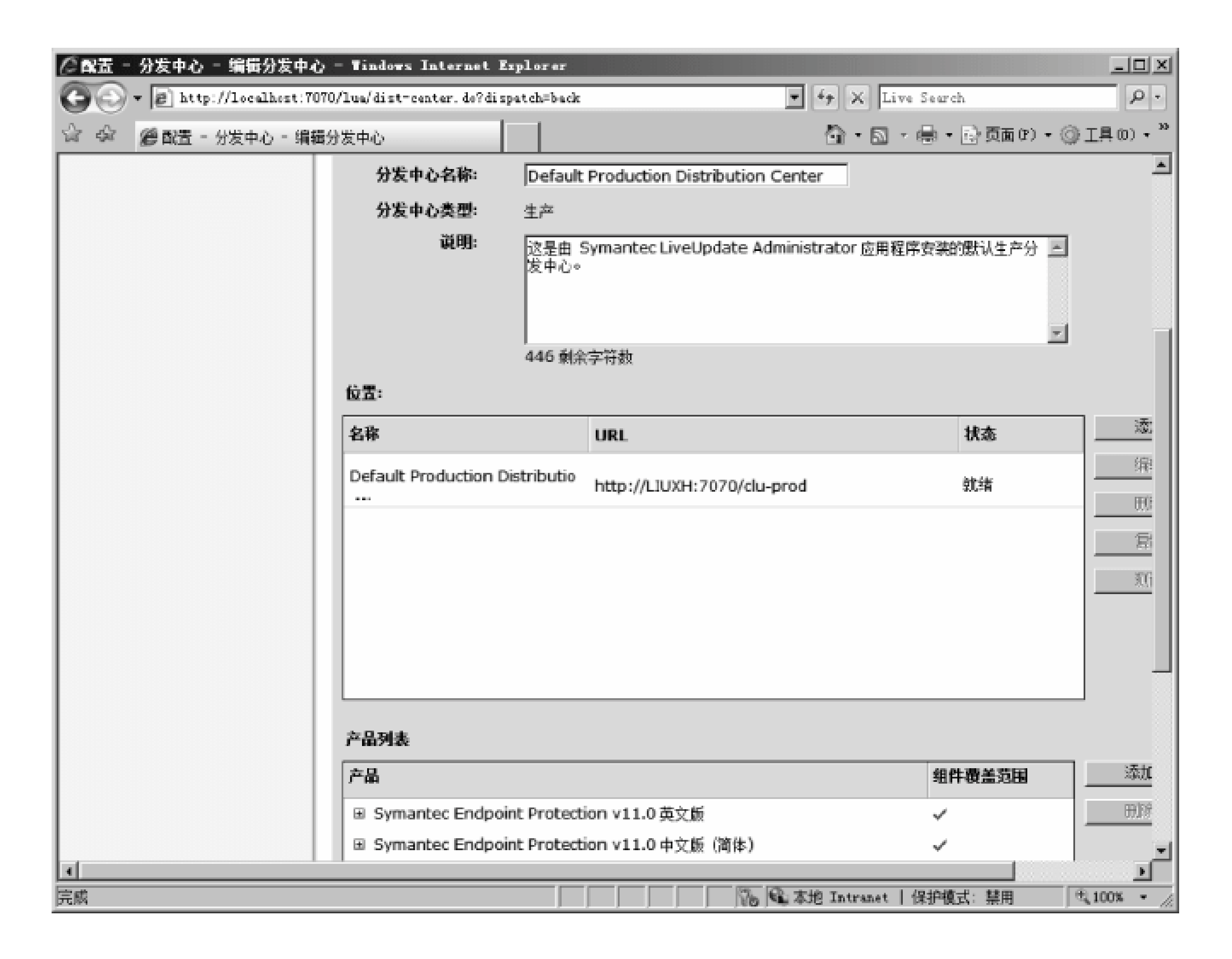


图 5-35　“编辑分发中心”窗口

提示: *如果不添加产品,则无法向客户端分发更新。*

(7) 在打开的“下载和分发”窗口中,选择已创建的分发调度,单击“立即运行”按钮,即可开始向客户端分发更新,如图 5-36 所示。分发完成后,单击“确定”按钮即可。



图 5-36　正在分发更新

5.5.3　配置 LiveUpdate 策略

配置 LiveUpdate 策略的操作步骤如下。

(1) 登录到“Symantec Endpoint Protection Manager 控制台”,单击“策略”按钮,在左侧

的“查看策略”窗格中选择 LiveUpdate 选项，显示如图 5-37 所示的“LiveUpdate 策略”窗口。



图 5-37 “LiveUpdate 策略”窗口

(2) 选择“LiveUpdate 设置策略”选项，右击并选择快捷菜单中的“编辑”选项，显示“LiveUpdate 策略”对话框。在左侧栏中选择“服务器设置”选项，显示如图 5-38 所示的“服务器设置”对话框。选中“使用 LiveUpdate 服务器”单选按钮，并选中“使用指定的内部 LiveUpdate 服务器”单选按钮。



图 5-38 “服务器设置”对话框

(3) 单击“添加”按钮，显示如图 5-39 所示的“添加 LiveUpdate 服务器”对话框。在“服务器名”文本框中输入 LiveUpdate 服务器的计算机名。在 URL 文本框中输入 LiveUpdate

服务器的地址，格式为“http://LiveUpdate 服务器名：7070”，例如 http://symantec.coolpen.net:7070。在“用户名和密码”文本框中输入 LiveUpdate 服务器的用户名和密码。

（4）单击“确定”按钮，添加成功，返回“服务器设置”对话框。继续单击“确定”按钮，LiveUpdate 策略设置完成。当在客户端运行 LiveUpdate 时，就会自动连接 LiveUpdate 服务器下载更新。



图 5-39 “添加 LiveUpdate 服务器”对话框

5.5.4 知识链接：LiveUpdate

1. Symantec LiveUpdate

LiveUpdate 是一种使用防病毒定义、入侵检测特征、产品补丁程序等内容来更新客户端计算机的实用程序。在非受管环境中，客户端计算机上的 LiveUpdate 通常会配置为直接连接至 Symantec LiveUpdate 服务器。在中小型网络的受管环境中，客户端计算机上的 LiveUpdate 通常会配置为连接到 SEP Manager。在大型受管网络中，通过 Internet 网关的带宽节约问题可能非常重要。当这些问题确实重要时，可以安装并配置一台或多台 LiveUpdate 服务器来下载更新。然后，用户可以将更新分发到管理服务器，或直接分发给客户端。

2. LiveUpdate 体系结构

图 5-40 所示是 Symantec LiveUpdate 的基本体系结构。通过配置 SEP 客户端的 LiveUpdate 选项，即可使其从局域网中的 LiveUpdate 服务器获取更新。LiveUpdate 服务器可以通过 3 种方式为 SEP 客户端提供更新，依据网络规模选择适当的方式即可，其中在 SEP 客户端和 LiveUpdate 服务器之间增加代理服务器的方式最复杂，适用于客户端较多的大型企业网络。

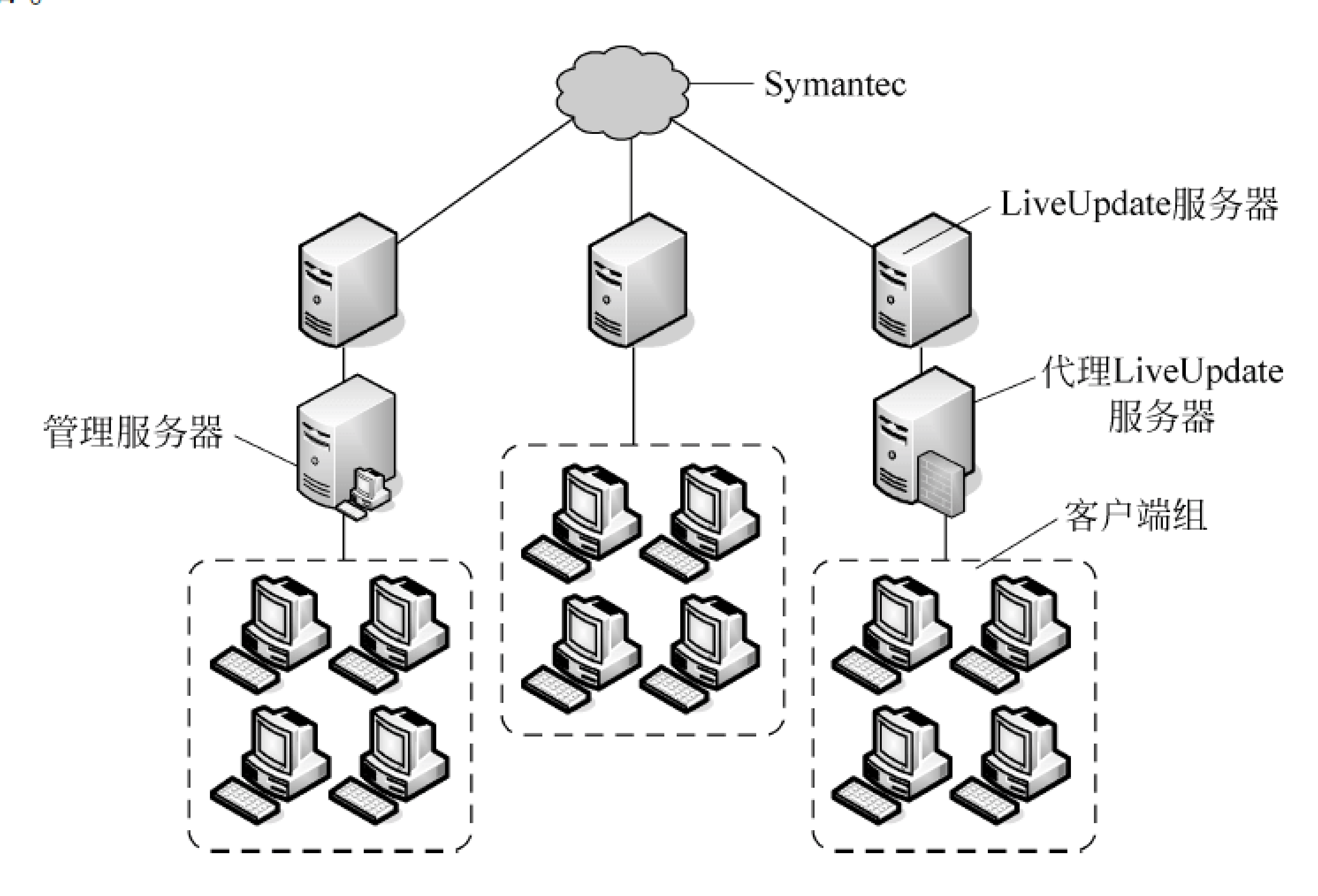


图 5-40 LiveUpdate 体系结构

5.6 客户端管理

部署网络防病毒系统的主要目的是便于实现对客户端的统一管理，例如软件更新、指定扫描计划、执行病毒扫描与查杀等。与单机防病毒软件最大的区别就是，所有的管理操作都可以由管理员在 SEP Manager 控制台上完成，而客户端无须进行任何操作，甚至不会影响客户端的正常工作。

5.6.1 配置管理策略

管理员对 SEP 客户端的管理都是基于策略实现的，默认情况下所有客户端分组均已被应用默认管理策略，包括 LiveUpdate 功能配置、防病毒软件配置、防火墙配置等。管理员可以通过更改默认策略，或者创建并应用新的策略，启用所需的管理方式。

(1) 在 SEP Manager 控制台窗口中，单击“客户端”标签，打开“查看客户端”窗口，选中希望配置管理策略的客户端组，切换至“策略”选项卡，显示如图 5-41 所示的窗口。默认情况下，系统已经自动选中“从父组"My Company"继承策略和设置”复选框，建议将其取消。

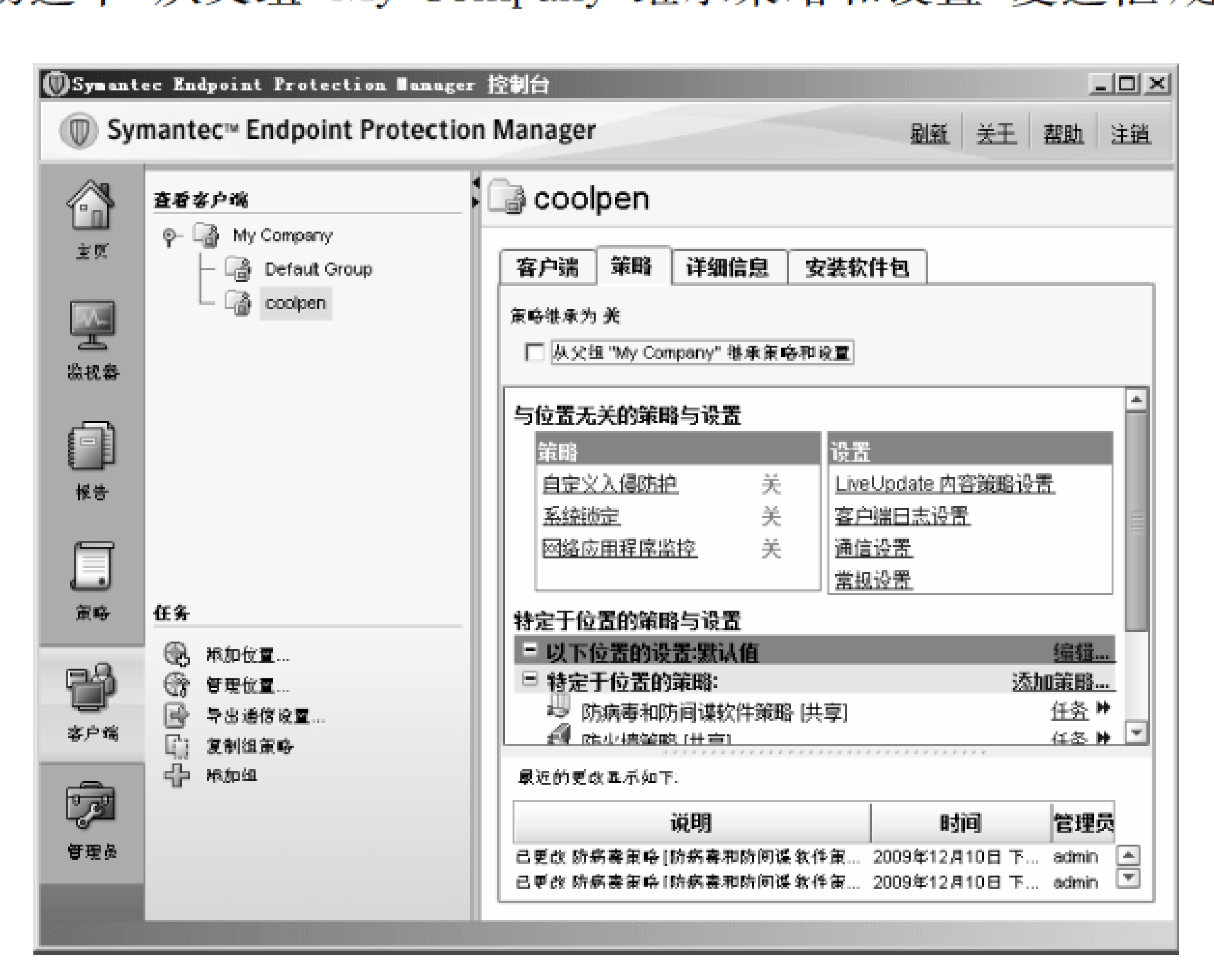


图 5-41 “策略”选项卡

(2) 在“特定于位置的策略与设置”列表中单击希望配置的策略，例如“防病毒和防间谍软件策略”，显示如图 5-42 所示的“编辑策略”对话框。提示该默认策略是共享策略，可能同时应用于多个组，如果直接单击“编辑共享”按钮，则将直接修改策略，并将修改结果应用于其他客户端组。如果单击“使用副本创建非共享策略”按钮，则仅对策略副本进行修改，修改结果也仅应用于当前组。

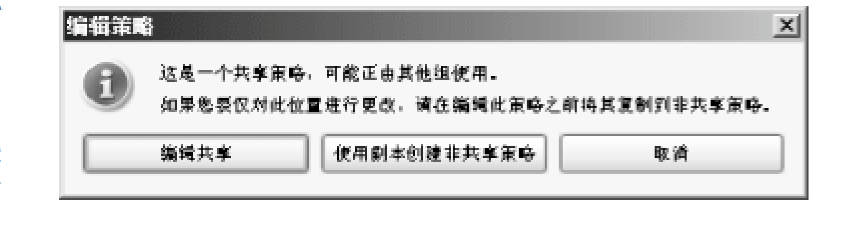


图 5-42 “编辑策略”对话框

(3) 单击“使用副本创建共享策略”按钮，显示如图 5-43 所示的“防病毒和防间谍软件策略”对话框，在“概述”选项卡中显示了策略名称和相关说明信息。选择“管理员定义的扫描”选项，在“扫描”选项卡中显示了默认的扫描调度，并且已启用。



图 5-43 “防病毒和防间谍软件策略”对话框

（4）单击“添加”按钮，显示“添加调度扫描”对话框，选中“创建新的调度扫描”单选按钮，单击“确定”按钮，显示如图 5-44 所示的“扫描详细信息”选项卡。在“扫描名称”文本框中输入新调度扫描的名称，在“扫描类型”下拉列表框中选择“全面扫描”选项，可用的扫描类型包括“全面扫描”、“活动扫描”和“自定义扫描”。

（5）单击“调度”标签，显示如图 5-45 所示的“调度”选项卡，配置执行扫描的频率和具体时间，以及错过调度扫描后重新执行扫描的时间。例如，此处设置为每天下午 5 点执行客户端扫描，如果客户端关机，则在 16 小时之后重试扫描。




图 5-44 “扫描详细信息”选项卡

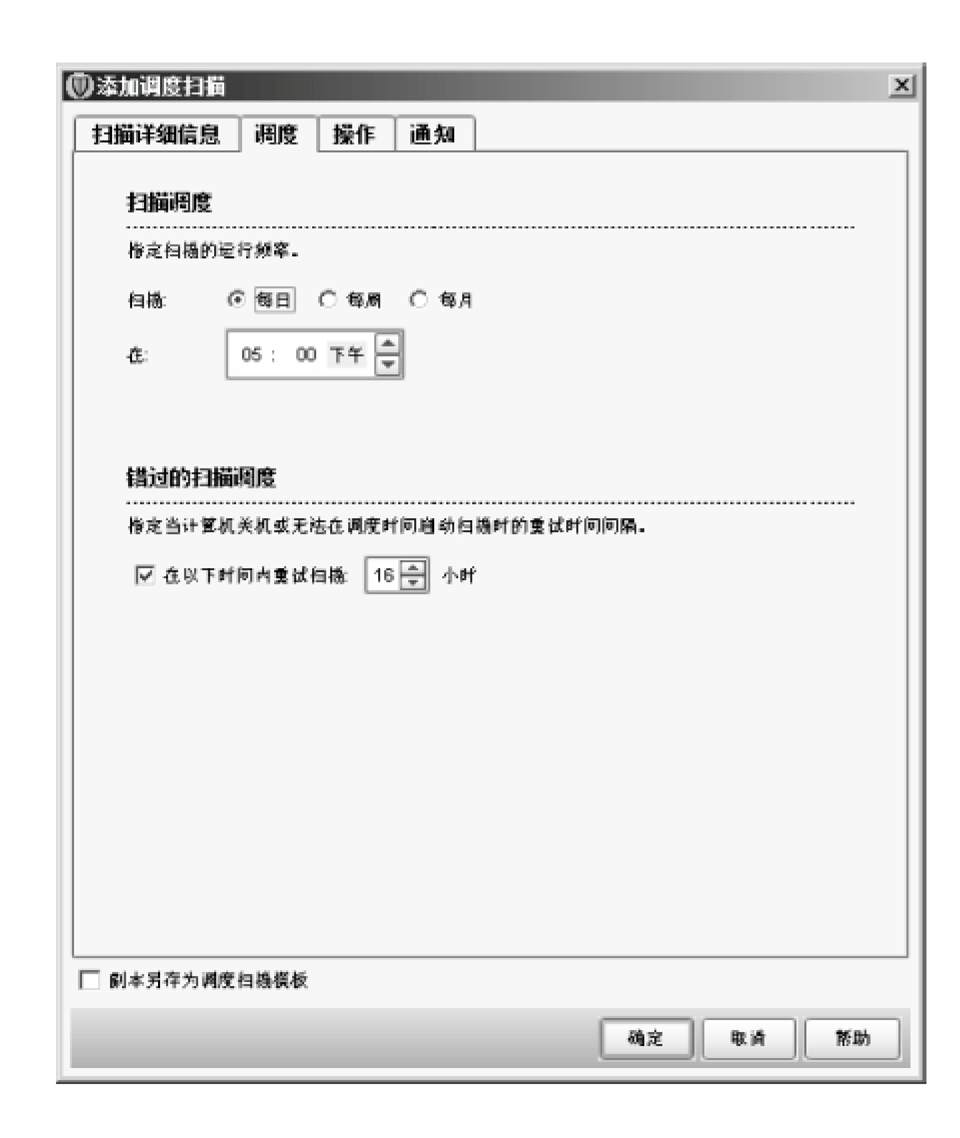


图 5-45 “调度”选项卡

(6) 单击“操作”标签，显示如图 5-46 所示的“操作”选项卡，可以设置针对各种病毒的处理操作，默认的第一操作为“清除风险”，如果清除风险失败，则还会尝试“隔离风险”，避免其感染其他文件。

(7) 单击“通知”标签，显示如图 5-47 所示的“通知”选项卡，选中“在受感染的计算机上显示通知消息”复选框。如果扫描过程中发现客户端计算机上的病毒，则显示相关提示信息，该信息是可以编辑的。



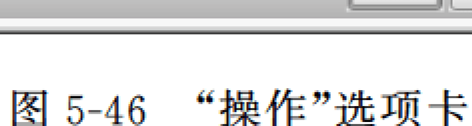


图 5-46 “操作”选项卡



图 5-47 “通知”选项卡

(8) 连续单击“确定”按钮，保存设置并返回“防病毒和防间谍软件策略”对话框，可以继续设置相关的其他操作，操作过程与此类似。其他管理策略的配置与“防病毒和防间谍软件策略”相同，这里不再赘述。

5.6.2 更新内容

对客户端执行“更新内容”操作，可以确保 SEP 客户端病毒库定义最新，使其可以识别并查杀最新型的计算机病毒。

在 SEP Manager 控制台窗口的“客户端”选项卡中，右击希望执行操作的客户端计算机，依次选择“对客户端运行命令”→“更新内容”选项，显示如图 5-48 所示的“更新内容”对话框，单击“是”按钮确定即可。

5.6.3 病毒扫描与查杀

在 SEP Manager 控制台窗口的“客户端”选项卡中，右击希望执行操作的客户端计算机，依次选择“对客户端运行命令”→“扫描”选项，显示“扫描”对话框，提示是否向客户端发送“扫描”命令，单击“是”按钮，显示如图 5-49 所示的“选择扫描类型”对话框，选择希望执行的扫描类型，单击“确定”按钮，客户端即可开始病毒扫描。

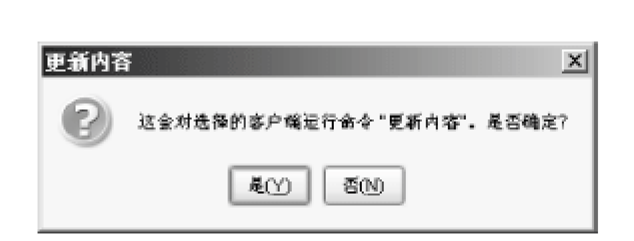


图 5-48 “更新内容”对话框

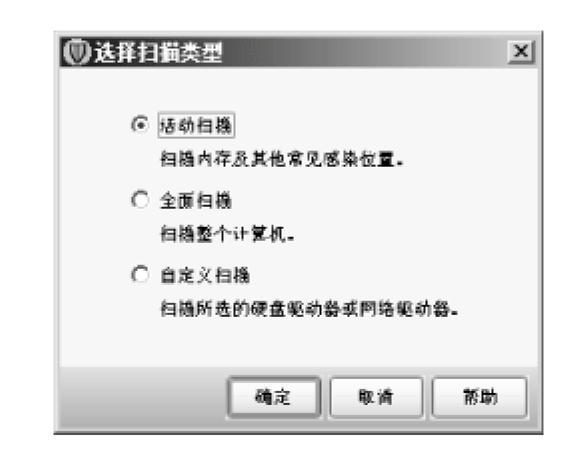


图 5-49 “选择扫描类型”对话框

5.6.4 在客户端执行病毒扫描

除了由管理员控制远程客户端的病毒扫描之外，客户端用户还可以随时进行活动扫描、全面扫描或自定义扫描。活动扫描只扫描最常感染病毒的区域；全面扫描可以对整个计算机进行扫描；自定义扫描则可以根据用户需求，对指定的目录或对象进行扫描。

(1) 在客户端计算机上打开 Symantec Endpoint Protection 窗口，切换到“扫描威胁”选项卡，如图 5-50 所示。



图 5-50 “扫描威胁”选项卡

(2) 单击希望进行的扫描类型即可开始扫描，例如单击“活动扫描”按钮，显示如图 5-51 所示的“活动扫描”窗口。扫描过程中如果发现病毒，则将显示在窗口的列表中，选中指定的对象，并单击“立即删除风险”按钮即可删除病毒。

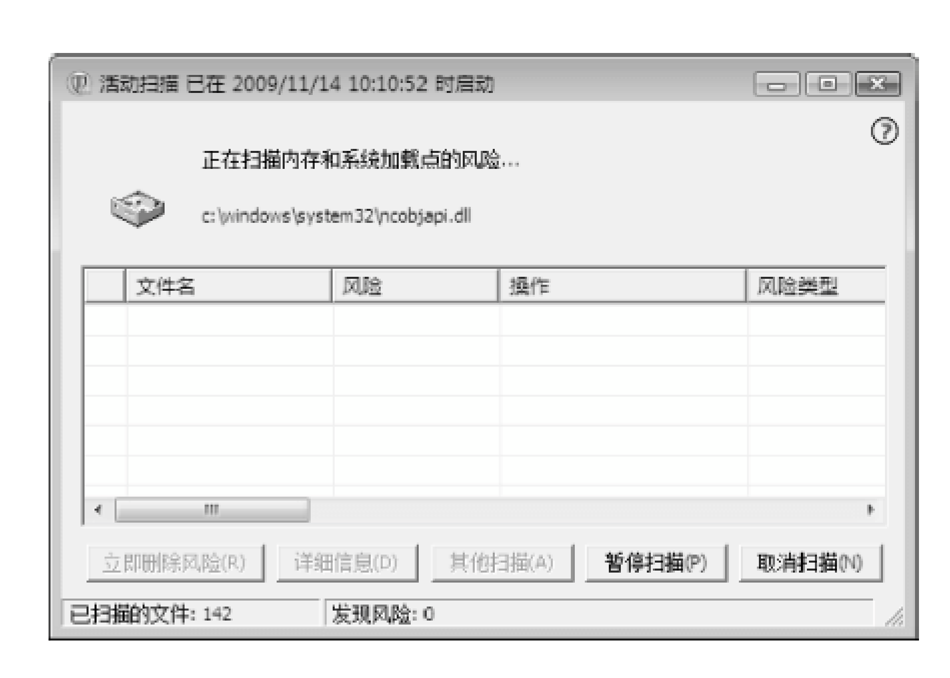


图 5-51 “活动扫描”窗口

5.6.5 知识链接：SEP 客户端

1. SEP 客户端管理任务

SEP 客户端的主要管理任务都是通过 SEP Manager 控制台实现的，可以对客户端执行的操作如下。

(1) 扫描。在客户端上运行按需扫描。

(2) 取消所有扫描。取消当前在客户端计算机上运行的全部扫描。

(3) 更新内容。在客户端上初始化 LiveUpdate 会话,以更新客户端的内容。客户端计算机会从 Symantec LiveUpdate 接收最新的内容。

(4) 更新内容并扫描。初始化 LiveUpdate 会话以更新内容,然后在客户端上运行按需扫描。

(5) 重新启动客户端计算机。

(6) 启用自动防护。在客户端启用"文件系统自动防护"。

(7) 启用网络威胁防护。在客户端启用"网络威胁防护"。

(8) 禁用网络威胁防护。在客户端禁用"网络威胁防护"。

2. SEP 客户端功能

防病毒和防间谍软件防护可确保计算机免遭已知病毒与安全风险的攻击。如果能够很快地从计算机中检测到病毒并将其删除,则可以阻止其感染到其他文件。当 Symantec Endpoint Protection 客户端检测到病毒或安全风险时,默认情况下客户端会通知用户检测的结果。如果不希望收到通知,则管理员可以将客户端配置为自动处理风险。防病毒和防间谍软件防护可提供以特征为基础的扫描,并包括下列功能。

(1) 自动防护扫描。自动防护会持续运行,并通过监控计算机上的活动为计算机提供实时防护。自动防护会在文件执行或打开时查看其是否含病毒或安全风险,也会在修改文件时查看其是否含病毒或安全风险。

(2) 调度、启动及按需扫描。管理员可以配置其他要在客户端计算机上运行的扫描。这些扫描会搜索受感染文件中残留的病毒特征,也会搜索受感染文件中安全风险的特征与系统信息。管理员都可以启动扫描,系统地检查计算机上的文件是否有病毒和安全风险。

习题

1. 简述计算机病毒的定义及其基本特征。
2. 最近几年爆发的计算机病毒有哪些共同特征?
3. 计算机病毒传播的主要途径有哪些?
4. 如何判定一台计算机可能感染了病毒?
5. 简述 SEP 网络防病毒系统的运行机制。

实验:通过各种方式部署 SEP 客户端

实验目的:

掌握 SEP 客户端的部署方法。

实验内容:

为不同环境中的客户端选择合适的 SEP 客户端安装方式,包括"推"式安装、查找安装和客户端手动安装。

实验步骤:

(1) 在域中部署备用的 SEP 服务器。

(2) 在客户端计算机上运行 ping 命令,分别测试到 SEP 服务器的连通性。

(3) 使用"推"方式为域中的指定计算机安装 SEP 客户端。

(4) 使用"查找"方式搜索企业网络中的计算机,选择用于实验的客户端并安装 SEP 客户端。

(5) 登录未加入域的客户端计算机,通过网络共享或其他方式获取 SEP 服务器生成的 SEP 客户端安装包。

(6) 运行安装包,部署 SEP 客户端。

(7) 登录 SEP Manager 管理控制台,检查是否能浏览到已部署的所有 SEP 客户端。

第 6 章 chapter 6

系统补丁更新

对于 Windows 操作系统而言，漏洞是在所难免的。随着用户的不断应用和发掘，各种各样的系统漏洞将不断涌现。应对系统漏洞最有效的措施就是及时安装系统补丁，即安装 Microsoft 网站发布的系统更新。如果网络中计算机数量较多，大量计算机同时更新还会占用大量 Internet 带宽。因此，可以通过部署 WSUS 服务器，可以从 Microsoft 网站下载所有的 Windows 更新，供局域网中的客户端下载安装，从而提高下载速度，并节省大量 Internet 带宽。

6.1 补丁管理规划

补丁主要是针对漏洞而言的，包括操作系统漏洞和应用程序漏洞等。对于一个中型企业网络而言，需要的网络服务多种多样，客户端技术水平参差不齐，安全漏洞的管理是非常必要的。

6.1.1 案例情景

目前，该企业网络中的服务器均使用 Windows 操作系统，网络服务提供程序也以 Microsoft 为主，客户端用户大部分使用 Windows Vista 或 Windows XP 系统，少量用户使用 Mac OS 或 Linux 操作系统。

网络中心的所有服务器均已开启自动更新功能，能够及时获取 Windows 或应用程序所需的补丁更新，弥补安全漏洞。但是，多台服务器同时下载较大的补丁文件时，对网络传输速率影响较大，导致正常访问无法顺利进行。客户端用户安全意识较差，大部分未启用 Windows 系统的自动更新功能，存在极大的安全隐患。一旦计算机病毒通过客户端系统漏洞入侵整个网络，后果将不堪设想。

6.1.2 项目需求

为服务器安装漏洞补丁自然是无可厚非的，但不应为此而影响正常的网络应用，尤其是重要的应用，如网络视频会议、即时通信等。问题的关键在于下载漏洞补丁产生的 Internet 流量上，企业网络的 Internet 连接带宽是有限的，如果多台服务器同时下载补丁，势必会占用大量的 Internet 带宽，而预留给其他网络应用的带宽就非常有限了，对 Internet 连接带宽需求较高的应用(例如网络会议)就会受到严重影响。如果可以降低由此产生的 Internet 带

宽开销,将下载漏洞补丁限制在网络内部,就可以解决这一问题。

对于客户端而言,也必须开启 Windows 系统的自动更新功能,以便及时获取系统和应用程序补丁。管理员可以通过组策略统一管理和配置客户端的更新功能。对于网络安全意识较差的用户要加强管理。

6.1.3　解决方案

可以在网络中部署专用的 WSUS(Windows Server Update Services)服务器,统一管理网络中计算机的漏洞补丁。内部用户可以通过 WSUS 服务器,集中从 Microsoft Update 网站下载更新程序,并且在完成这些更新程序的测试工作,确定对企业内部计算机不会有不良影响后,再通过管理员的核准程序,将这些更新程序部署到客户端的计算机上,如图 6-1 所示。

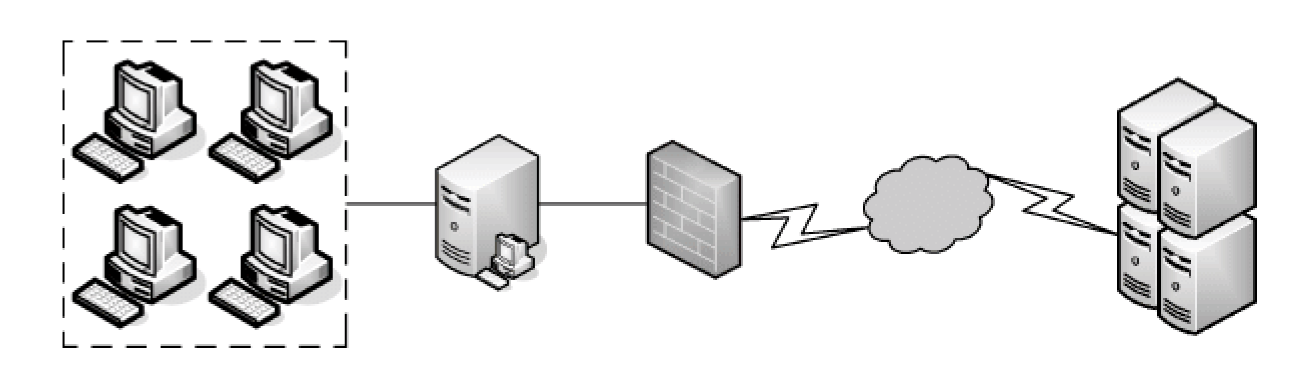


图 6-1　WSUS 运作模式

如果网络中的客户端计算机较多,则为了便于管理可以预先进行适当分组,可以更容易、更准确地将更新部署到指定的计算机上。默认情况下,安装和配置 WSUS 服务器的过程中,已经创建了两个分组,分别是所有计算机和未指派的计算机。客户端计算机在第 1 次跟 WSUS 服务器接触时,系统默认会将该计算机同时加入到这两个组内。在应用过程中,管理员也可以根据实际情况创建新的计算机分组,并在组之间灵活移动客户端计算机。

由于 WSUS 服务器是从 Microsoft Update 网站所下载的更新程序,最好经过测试后,再将其部署到客户端计算机,因此应建立一个测试计算机组,可以先将更新程序部署到测试计算机组内的计算机,待测试无误,确定对企业内部计算机不会有不良影响后,再将其部署到其他组内的计算机。

6.2　WSUS 概述

为了让用户的 Windows 系统与其他 Microsoft 产品能够更安全、更稳定、功能更强,因此 Microsoft 会不定期在网站上释出最新的更新程序(Update,例如 Hotfix、Service Pack 等)供使用者下载与安装,而一般使用者可以通过以下两种方式获取更新程序。

(1) 手动连接 Microsoft Update 网站。

(2) 通过 Windows 系统的自动更新功能。

然而企业内部不论是采用哪一种方式,都可能会有以下的缺点。

(1) 影响网络效率。如果企业内部每一台计算机都自行上网更新,则可能会增加对外网络的负担、影响对外联机的网络效率。

(2) 与现有软件相互干扰。若企业内部所使用的软件与更新程序有冲突,则用户下载

与安装更新程序可能会影响该软件或更新程序的正常运作。

6.2.1 WSUS 系统需求

WSUS 3.0 SP2 对服务器操作系统版本的要求如下。

（1）WSUS 服务器必须运行 Windows Server 2003、Windows Server 2008、Windows Vista 或 Windows XP SP3 系统，Windows 2000 系统不支持 WSUS 3.0。

（2）在安装 WSUS 服务之前，服务器不能安装终端服务。

WSUS 3.0 SP2 对服务器文件系统的需求如下。

（1）磁盘分区使用 NTFS 文件系统。

（2）系统分区中有至少 1GB 的磁盘空间。

（3）存储数据库文件的卷上有至少 2GB 的磁盘空间。

（4）存储内容的卷上至少要有 6GB 的磁盘空间。

（5）不能在压缩驱动器上安装 WSUS 3.0 SP2。

在 WSUS 服务器上，必须安装如下组件。

（1）安装 IIS，启动 Web 服务。

（2）Microsoft .NET Framework 2.0。

（3）Microsoft Report Viewer 2008 SP1 Redistributable。

WSUS 客户端的要求比较低，只要能正常运行客户端操作系统，并且能够连接 WSUS 服务器即可。除了 Windows 9x 系统以后，Windows 2000 及其以后的系统都支持通过 WSUS 获取系统更新。

WSUS 3.0 SP2 支持 Microsoft 公司全部产品的更新，不仅支持 Windows 2000 及其以后的所有 Windows 操作系统，例如 Windows 2000、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 等，还提供了对 Office、SQL Server、MSDE 和 Exchange Server 等内容的更新支持。

6.2.2 WSUS 服务器的架构

在客户端较少的网络中，使用一台 WSUS 服务器就足够了，如果客户端数量较多，则需要部署多台 WSUS 服务器，以降低服务器的负载，此时这些 WSUS 服务器之间就必须按照一定的架构进行部署，以提高资源利用率。在多台 WSUS 服务器的网络中，首先应选定一台 WSUS 服务器作为主服务器，使其可以直接从 Microsoft Update 网站获取更新程序。其他 WSUS 服务器并不直接连接 Microsoft Update 网站，而是从上游的主服务器来取得更新程序，如图 6-2 所示。

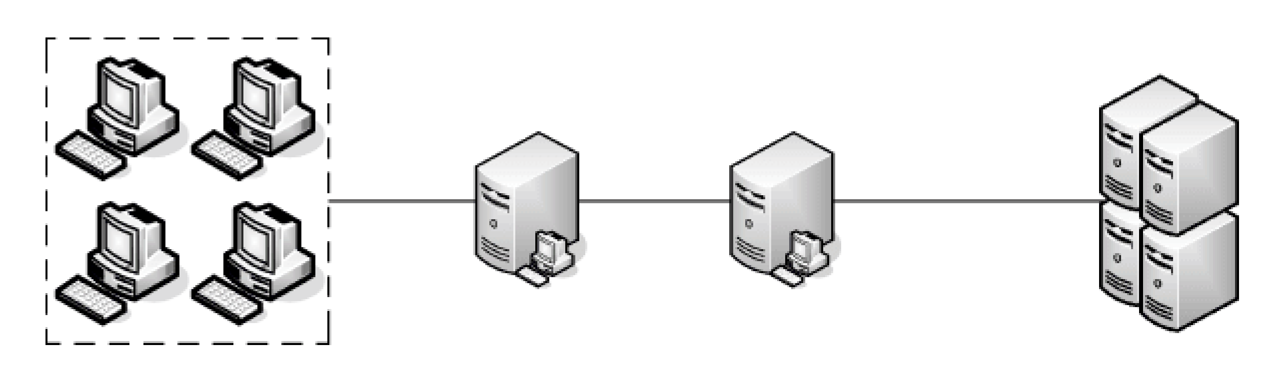


图 6-2　多台 WSUS 服务器的网络

通常情况下，用户可以通过如下两种方式配置多台 WSUS 服务器之间的协同工作。

1. 自治模式

上游 WSUS 服务器会与下游服务器共享更新程序，即下游 WSUS 服务器会从上游服务器获取更新程序，但是并不包含更新程序的核准状态、计算机分组信息，因此下游服务器必须自行决定是否要核准这些更新程序与自行建立所需的计算机组。

2. 复本模式

上游 WSUS 服务器会与下游服务器共享更新程序、更新程序的核准状态与计算机组信息，即下游 WSUS 服务器是从上游服务器获取上述信息，所有可以在上游服务器上管理的项目均无法在下游服务器自行管理，例如不能够自行改变更新程序的核准状态等。

注意：上述的计算机分组信息只有计算机分组本身而已，并不包含计算机群组的成员，用户必须手动在下游服务器来管理组成员；而客户端计算机在第 1 次跟下游 WSUS 服务器通信时，这些计算机默认是会被同时加入到所有计算机与尚未指派的计算机组内。

管理员可以根据实际网络环境和客户端需求，选择适当的部署方式。例如，只要从上游服务器下载一次更新程序，然后将它分配给位于分公司的下游服务器，以便降低互联网联机的负担。另外，应当注意的是，上游 WSUS 服务器不仅需要满足本地客户端更新程序的需求，还应考虑下游 WSUS 服务器的客户端的需求。例如，如果上游 WSUS 服务器的客户端仅需要简体中文版的更新程序，而下游 WSUS 服务器的客户端还需要英文的更新程序，则上游 WSUS 服务器必须同时下载简体中文版和英文版的更新程序。

注意：上下游 WSUS 服务器之间的连接方式，建议不要超过 3 层，因为每增加一层，就会增加延迟时间，因而拉长将更新程序传递到每一台服务器的时间。

6.2.3 WSUS 数据库

WSUS 服务可以使用 Windows Server 2008 系统内置的数据库，也可以使用 SQL Server 2005/2008 数据库。每一台 WSUS 服务器都有一个独立的数据库，用于存储如下信息。

(1) WSUS 服务器的配置信息。

(2) 描述每一个更新程序的数据表单(Metadata)。Metadata 内包含着以下信息。

① 更新程序的属性：例如更新程序的名称、描述、相关的技术库文章编号等。

② 适用规则：用来判断更新程序是否适用于某台计算机。

③ 安装信息：例如安装时所需的指令行参数。

(3) 客户端计算机及其与更新程序之间的关系等信息。

需要注意的是，数据库中并不会存储更新程序文件，因此还必须另外再选择更新程序的存储目录，用户可以从如下两种方式中选择。

1. 储存在 WSUS 服务器

此时 WSUS 服务器会从 Microsoft Update 网站(或上游服务器)下载更新程序，并将其储存到本地计算机。此种方式让客户端可以直接从 WSUS 服务器来取得更新程序，不用到 Microsoft Update 网站下载，如此便可以节省 Internet 连接带宽。

WSUS 服务器的硬盘必须要有足够的空间来储存更新程序档案，最少要有 20GB 的可用空间，建议是 30GB 以上，不过实际需求要看 Microsoft 提供的更新程序数量、下载的语言数量、产品的种类数量等因素而可能需要预留更多的可用空间。

2. 储存在 Microsoft Update 网站

此时 WSUS 服务器并不会从 Microsoft Update 网站来下载更新程序，换句话说，当用户执行 WSUS 服务器与 Microsoft Update 之间的同步工作时，WSUS 服务器只会从 Microsoft Update 网站下载更新程序的 Metadata 数据，并不会下载更新程序本身。

因此当管理员核准客户端可以安装某个更新程序后，客户端是直接连接 Microsoft Update 网站来下载更新程序。如果客户端计算机的数量不多，或是客户端与 WSUS 服务器之间的连接速度不快，但是却与 Internet 之间的连接速度较快时，就可以选择这种方式。

6.3　安装和配置 WSUS 服务器

WSUS 是 Microsoft 推出的网络化补丁分发方案，Windows Server 2008 已经集成了 WSUS 服务，可以集中下载所有 Microsoft 产品的更新程序。对于客户端计算机而言，不必再连接到 Microsoft 网站，直接从网络中配置的 WSUS 服务器上即可下载并安装更新程序，速度非常快，而且可以为网络节省 Internet 带宽。

6.3.1　安装 WSUS 服务器

由于 WSUS 3.0 已经集成在 Windows Server 2008 系统中，因此，不需专门从 Microsoft 网站下载，利用"添加角色向导"即可安装。不过，由于在安装过程中需要连接 Microsoft 网站并下载应用程序，因此，WSUS 服务器必须已经连接到 Internet。WSUS 安装完成后，会启动配置向导，用来完成一系列的配置工作。

1. 安装 WSUS 服务器

(1) 以管理员账户登录到 WSUS 服务器以后，在"服务器管理器"中启动"添加角色向导"，单击"下一步"按钮，显示如图 6-3 所示的"选择服务器角色"对话框。选中 Windows Server Update Services 复选框，同时会显示"是否添加 Windows Server Update Services 所需的角色服务"对话框，单击"添加所需的角色服务"按钮，同时安装 Windows Server Update Services 和"Web 服务器"。

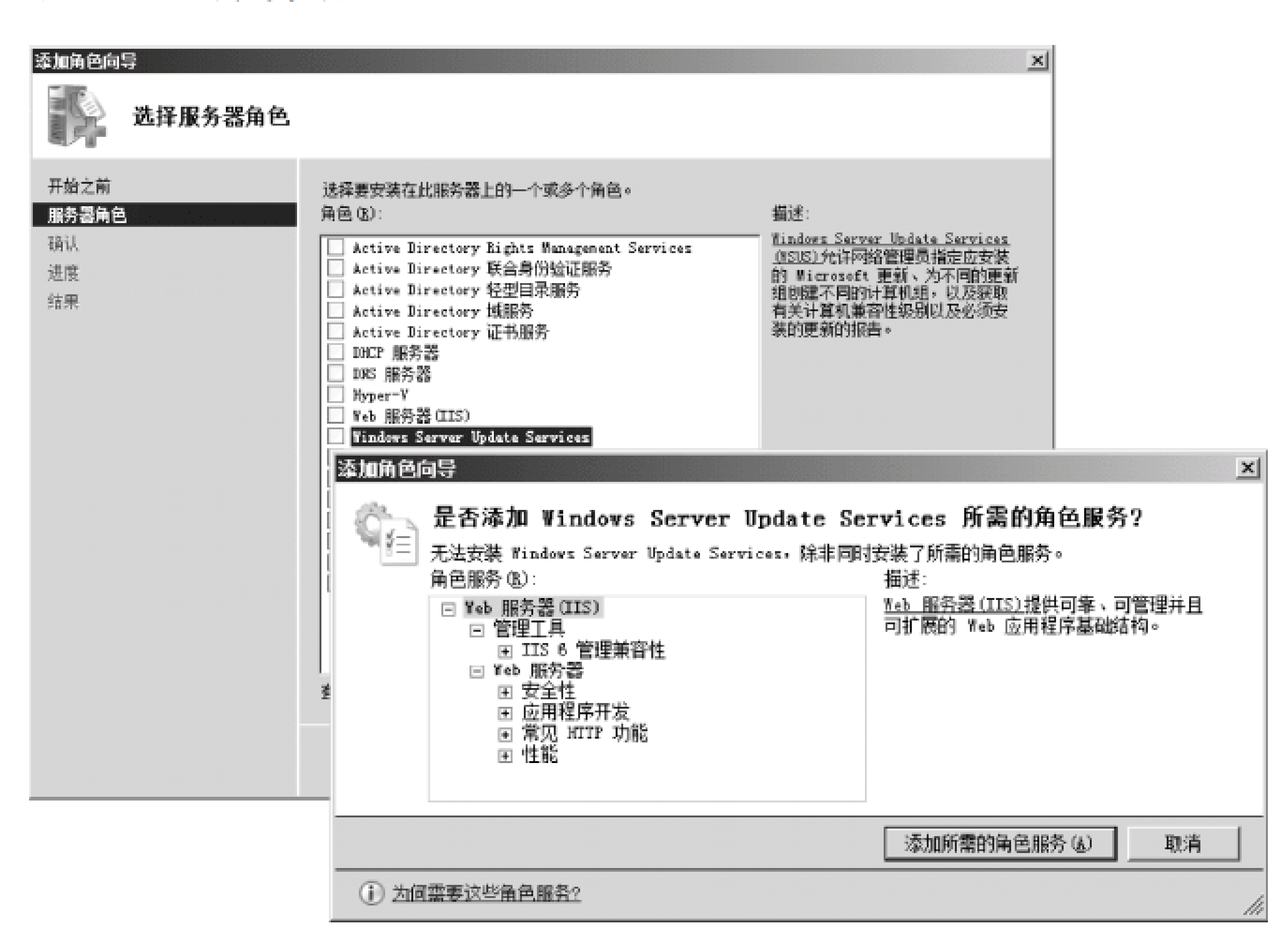


图 6-3　"选择服务器角色"对话框

(2) 单击“下一步”按钮，显示“Web 服务器(IIS)”对话框，提示 Web 服务器的简介信息。单击“下一步”按钮，显示如图 6-4 所示的“选择角色服务”对话框，用于选择 Web 服务器的组件。保持默认值即可。



图 6-4　“选择角色服务”对话框

(3) 连续单击“下一步”按钮，显示“确认安装选择”对话框。单击“安装”按钮开始安装，便会自动连接 Internet 并下载 WSUS 安装程序。下载完成后自动启动 WSUS 3.0 SP2 安装向导。直接单击“下一步”按钮，显示如图 6-5 所示的“许可协议”对话框。选中“我接受许可协议条款”单选按钮，接受许可协议。

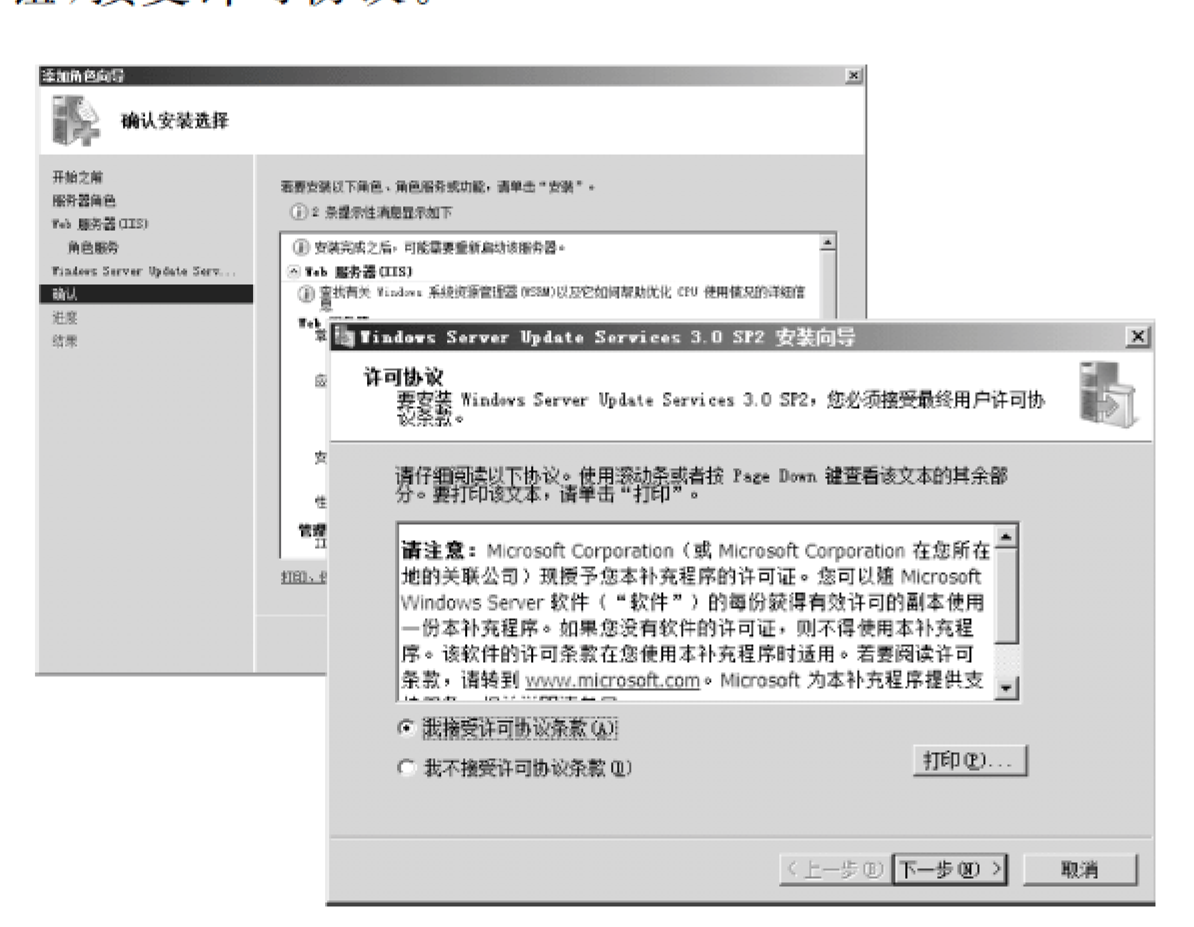


图 6-5　“许可协议”对话框

提示：如果当前服务器没有连接 Internet，则安装将不能成功。

(4) 单击“下一步”按钮，显示“选择更新源”对话框，用来设置更新程序在本地计算机上的存储位置。选中“本地存储更新”复选框，并设置一个保存路径即可。单击“下一步”按钮，显示如图 6-6 所示的“数据库选项”对话框，用于设置 WSUS 数据库的存储位置。通常，与系统更新保存在同一位置即可。

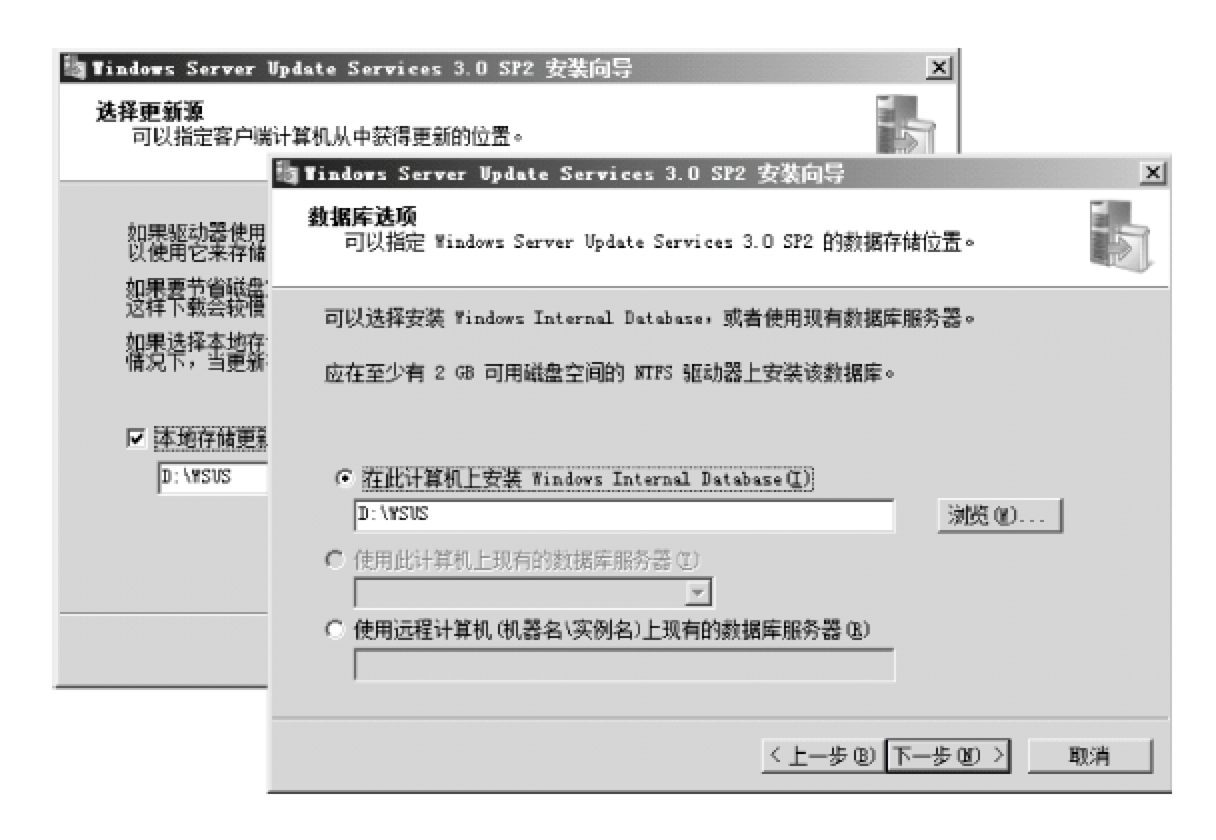


图 6-6 “数据库选项”对话框

注意：保存系统更新的磁盘尽量为非系统分区，并且至少有 6GB 的空间。

(5) 单击“下一步”按钮，显示如图 6-7 所示的“网站选择”对话框，WSUS 需要创建一个 Web 站点以供客户端计算机访问。如果当前服务器不配置为其他 Web 网站，选中“使用现有 IIS 默认网站(推荐)”单选按钮即可。如果当前服务器要为其他服务提供 Web 网站功能，则需选中“创建 Windows Server Update Services 3.0 SP2 网站”单选按钮。



图 6-7 “网站选择”对话框

(6) 单击“下一步”按钮，显示“准备安装 Windows Server Update Services 3.0 SP2”对话框，列出了前面所做的配置。继续单击“下一步”按钮，开始安装 WSUS，显示“正在完成 Windows Server Update Services 3.0 SP2 安装向导”对话框。单击“完成”按钮，返回“添加角色向导”，显示如图 6-8 所示的“安装结果”对话框，提示 WSUS 和 Web 服务器已安装完成。



图 6-8 “安装结果”对话框

(7) 单击“关闭”按钮，退出向导，WSUS 服务器安装完成，并自动启动配置向导，用来配置 WSUS。

2. WSUS 3.0 配置向导

当使用“添加角色向导”安装完 WSUS 以后，会立即启动 WSUS 配置向导，用来配置 WSUS 的同步方式、同步计划、所更新的产品和分类等。如果不想立刻配置，也可以将其取消，以后第一次启动 WSUS 时，或者在 WSUS 的控制台中，可以再次启动 WSUS 配置向导。

(1) 退出 WSUS 向导时，即可启动 WSUS 配置向导。单击“下一步”按钮，显示“加入 Microsoft Update 改善计划”对话框，选择是否加入 Microsoft Update 改善计划。单击“下一步”按钮，显示如图 6-9 所示的“选择‘上游服务器’”对话框。选中“从 Microsoft Update 进行同步”单选按钮，从 Microsoft 网站进行同步；但如果网络中已经配置有 WSUS 服务器，可以选中“从其他 Windows Server Update Services 服务器进行同步”单选按钮，并输入上游 WSUS 服务器的 IP 地址，从已有的 WSUS 服务器同步更新。



图 6-9　“选择‘上游服务器’”对话框

(2) 单击“下一步”按钮，显示“指定代理服务器”对话框，用来设置代理服务器。如果不需要代理，则不需设置。单击“下一步”按钮，显示“连接到上游服务器”对话框，需要连接上游服务器并下载同步更新的信息。单击“开始连接”按钮，开始连接上游服务器并下载相关信息，如图 6-10 所示。

(3) 单击“下一步”按钮，显示“选择‘语言’”对话框，需要选择网络中使用的更新语言。通常选中“中文(简体)”复选框即可。如果网络中也使用了英文版的系统或者应用程序，则需同时选中“英语”复选框。单击“下一步”按钮，显示“选择‘产品’”对话框，需要选择更新的产品。应根据网络中所使用的操作系统和应用程序版本来选择。单击“下一步”按钮，显示“选择‘分类’”对话框，指定要同步的更新分类。图 6-11 所示为设置更新语言、产品和分类。

(4) 单击“下一步”按钮，显示“设置同步计划”对话框，设置如何与上游服务器同步。为了方便管理，减少管理员的操作，建议选中“自动同步”单选按钮，并设置同步时间和次数，使

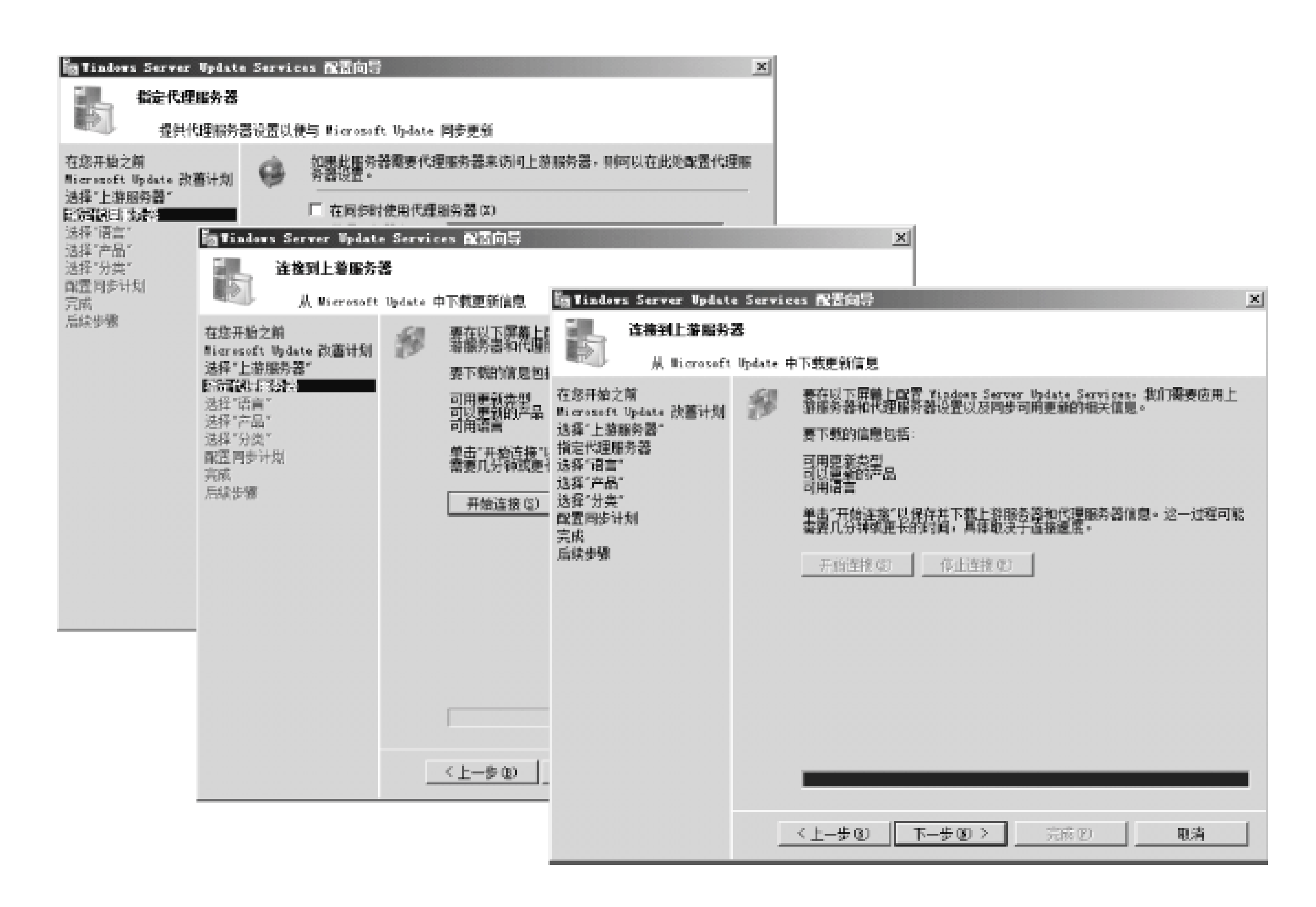


图 6-10　连接上游服务器

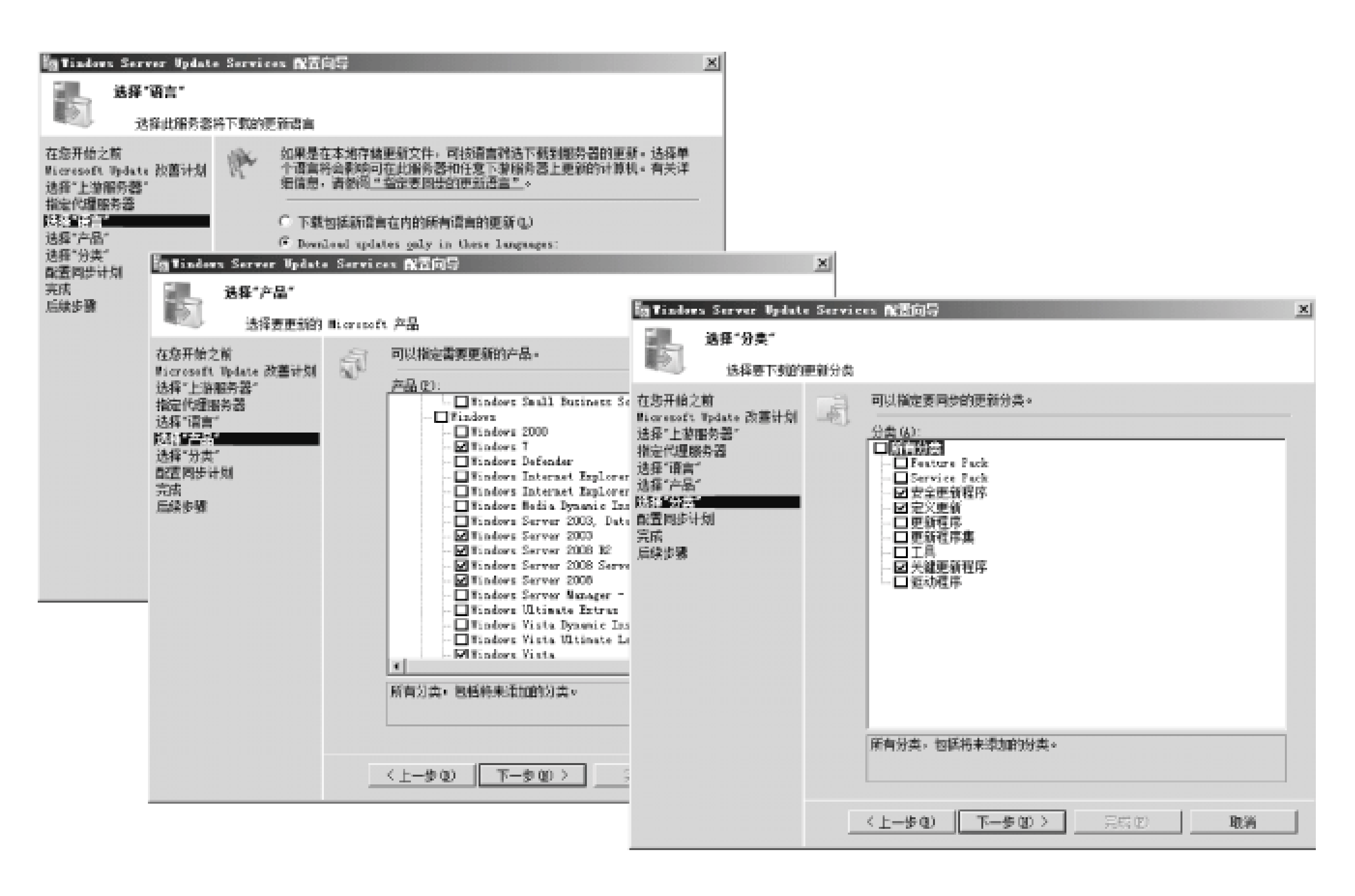


图 6-11　设置更新语言、产品和分类

服务器自动同步。单击“下一步”按钮，显示“完成”对话框。选中“开始初始同步”复选框，准备在完成后进行第一次同步。单击“下一步”按钮，显示如图 6-12 所示的“后续步骤”对话框，列出了完成配置的后续操作。

（5）单击“完成”按钮，安装完成。

依次选择“开始”→“管理工具”→Windows Server Update Services 选项，打开 WSUS 控制台，显示如图 6-13 所示的 Update Services 窗口。在该窗口中即可管理 WSUS。

6.3.2　配置 WSUS 服务器

WSUS 服务器安装完成后并不能立即投入使用，必须根据实际环境和需求进行合理配置，如 Internet 接入方式、获取更新、客户端分配、系统更新的审批等。同时，管理员也需要经常查看 WSUS 的更新报告，以便了解所有的更新信息。

1. 同步

“同步”就是当前 WSUS 服务器从 Microsoft Update 站点或其上游 WSUS 服务器获取

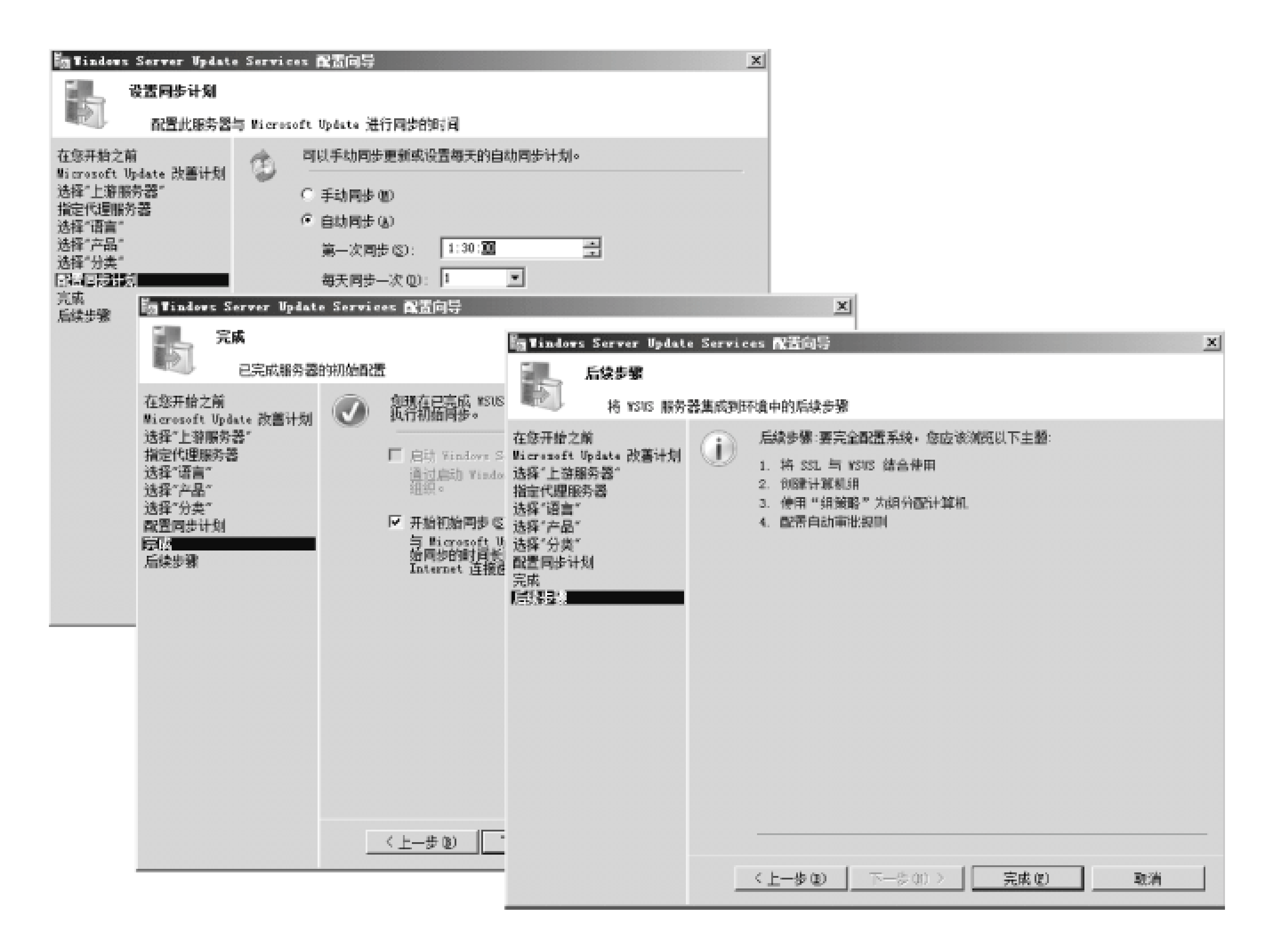


图 6-12　“后续步骤”对话框



图 6-13　Update Services 窗口

更新的过程。同步有手动同步和自动同步两种方式，应根据网络的使用情况来决定何时进行同步。通常使用自动同步，并将同步计划设置为访问 Internet 较少的时间段，例如凌晨。如果网络带宽资源紧张，则可使用手动同步方式。

(1) 在 WSUS 控制台窗口，选择“同步”选项，显示如图 6-14 所示的窗口，列出了最近执行过的同步操作。单击一个同步信息，在“同步详细信息”框中可以显示该次同步的启动时间、完成时间、结果、类型等。

(2) 单击“操作”列表中的“立即同步”链接，即可开始同步，并在“同步状态”框中显示当前的同步状态及进度。

2. 计算机

在“选项”设置窗口中，单击“计算机”链接，打开如图 6-15 所示的“计算机”对话框。管理员可以通过两种方法为计算机组分配计算机：WSUS 控制台设置和客户端策略设置。使



图 6-14 “同步”窗口

用服务器端设置时，可使用 WSUS 管理控制台将客户端计算机移到计算机组中（每次移到一个计算机组）。使用客户端策略设置时，可在客户端计算机上使用组策略或编辑注册表设置，以便将这些计算机自动添加到计算机组中。

提示：两种分配方法只能任选其一。

3. 自动审批

（1）在选项列表中单击“自动审批”链接，显示“自动审批”对话框。单击“新建规则”按钮，显示如图 6-16 所示的“添加规则”对话框。首先在“步骤 1：选择属性”列表框中，选择希望用于批准特定分类的更新还是审批用于特定产品的更新；选中某一项前面的复选框的同时，在“步骤 2：编辑属性（单击带下划线的值）”列表框中也会自动增加针对该项的详细设置；在“步骤 3：指定名称”文本框中输入新规则的名称。



图 6-15 “计算机”对话框



图 6-16 “添加规则”对话框

（2）在“步骤 2：编辑属性（单击带下划线的值）”编辑分类列表框中，还可以对选定的分类进行详细编辑。例如单击“任何分类”链接，打开如图 6-17 所示的“选择‘更新分类’”对话框。默认状态下，列表中的所有产品都是被选中的，有些产品类型并不是需要的，只须在这里将其取消选中即可。

(3) 单击“确定”按钮,保存设置并返回“自动审批”对话框,如图 6-18 所示。



图 6-17 “选择‘更新分类’”对话框



图 6-18 “自动审批”对话框

(4) 选中成功创建的审批规则后,单击“运行规则”按钮,打开如图 6-19 所示的“运行规则”对话框,提示用户启用规则之前需要先进行保存,以及是否要继续。

(5) 单击“是”按钮即可开始运行,此时 WSUS 服务器会根据所选自动批准规则中的限制和过滤条件,筛选可用的更新安装程序,可能需要等待一段时间。成功完成后,显示如图 6-20 所示结果,提示被自动批准的更新的数量。

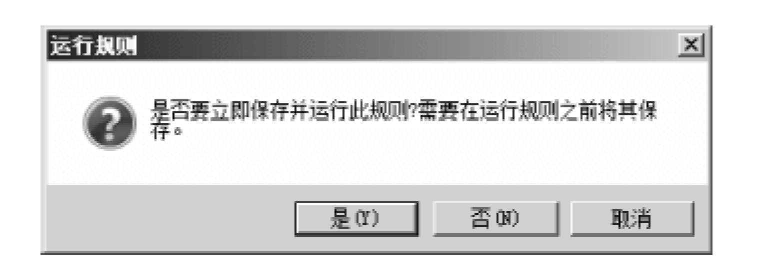


图 6-19 “运行规则”对话框



图 6-20 “正在运行规则”对话框

(6) 单击“关闭”按钮,保存设置即可。

在“自动审批”对话框中,单击“高级”切换至如图 6-21 所示的“高级”选项卡,默认情况下,系统自动审批 WSUS 更新和更新修订,并自动拒绝过期的更新,用户也可以根据实际需要暂时将其取消。

4. 报告汇总

该选项只适用于存在下游服务器的 WSUS 服务器。在“选项”设置窗口中,单击“报告汇总”链接,打开如图 6-22 所示的“报告汇总”对话框。系统默认选中“从副本下游服务器汇总状态”单选按钮,即自动收集来自下游 WSUS 服务器的状态信息。最后,单击“确定”按钮保存设置即可。

5. 电子邮件通知

启用 WSUS 服务器的 E-mail 功能后,服务器可以在完成同步后第一时间通知管理员,或者直接将收集到的状态报告发送给管理员,以备日后查询和调用。单击“电子邮件通知”链接,打开如图 6-23 所示的“电子邮件通知”对话框,默认显示“常规”选项卡。选中“在同步新更新时发送电子邮件通知”复选框,并在“收件人”文本框中输入收件人的 E-mail 地址;选中“发送状态报告”复选框,然后分别对发送频率和发送时间进行设置即可,如果需要同时向多个用户发送电子邮件通知,则可以在“收件人”文本框中同时输入多个 E-mail 地址,并以逗号分隔;在“语言”下拉列表框中,还可以选择电子邮件内容使用的语言类型。



图 6-21 “高级”选项卡



图 6-22 “报告汇总”对话框

单击“电子邮件服务器”切换至如图 6-24 所示的“电子邮件服务器”选项卡。由于发送邮件的过程是由 WSUS 服务器自动完成的,所以这里还要对发送邮件时使用的用户名和邮件服务器进行设置。设置完毕后,可以先单击“测试”按钮,测试一下指定的收件人是否确定可以收到 WSUS 服务器发送的邮件通知,确认成功后再单击“应用”按钮保存设置。

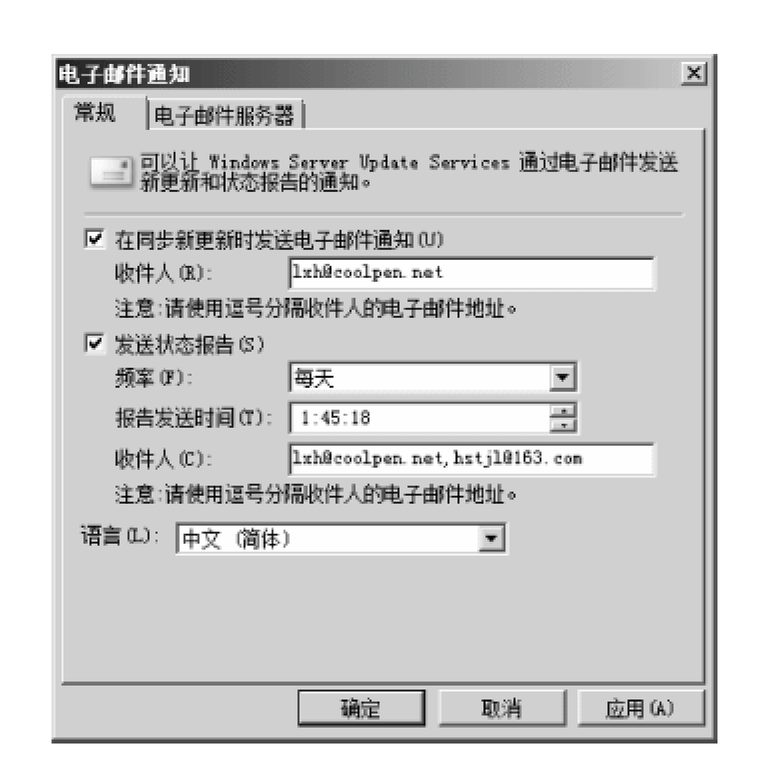


图 6-23 “电子邮件通知”对话框



图 6-24 “电子邮件服务器”选项卡

6.3.3 管理 WSUS 服务器

WSUS 服务器的日常管理和维护是至关重要的,原因很简单,由于 WSUS 服务器担负着众多客户端系统更新的重要任务,随时需要下载更新,并将其发送到指定的客户端,随着时间的推移,难免会因为系统中的垃圾文件过多而降低运行速度。因此,管理员应根据客户端变化情况,随时调整 WSUS 服务器的下载任务和运行状态,并定期删除旧的更新程序。

1. 计算机及分组管理

WSUS 对客户端的管理都是通过分组的方式进行的,分组标准非常灵活,可以根据所需更新类型的不同划分,也可以根据所属部门的不同进行划分,还可以删除多余分组。默认情况下,所有 WSUS 客户端都将存储在“未分配的计算机”分组中,管理员可以根据需要将其迁移或复制到其他分组。例如,在实施广泛分发更新之前必须对部分客户端进行测试,确保不会发生任何意外的情况后,才可以分发安装到所有客户端,此时就应创建一个临时组或测试组。

(1) 管理计算机分组

在 Update Services 窗口中，右击“所有计算机”并选择快捷菜单中的“添加计算机组”选项，打开如图 6-25 所示的“添加计算机组”对话框，在“名称”文本框中输入计算机组的名称，如 test。单击“添加”按钮，即可添加到默认的“所有计算机”组中。

如果当前分组中的客户端数量非常多，为了便于查看和管理，可以先按照一定的规则将其分类，例如名称、IP 地址、操作系统类型等。如果需要删除计算机分组，则可以在 Update Services 窗口中，右击分组名称(如 test)，并选择快捷菜单中的“删除”选项，打开如图 6-26 所示的“删除计算机组”对话框。这里包括 3 个单选按钮。



图 6-25　“添加计算机组”对话框

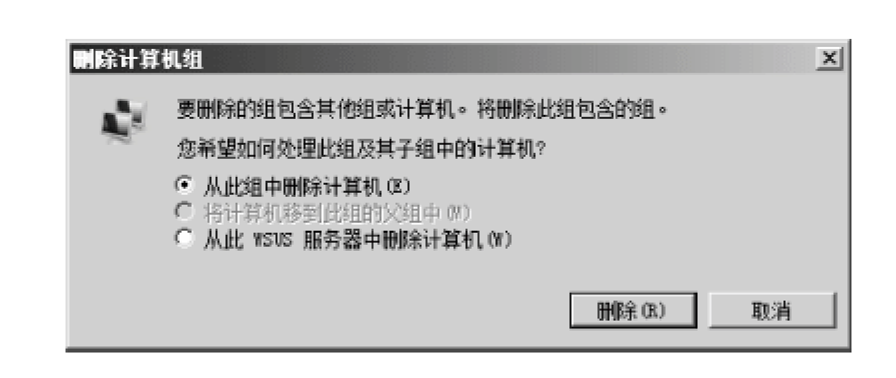


图 6-26　“删除计算机组”对话框

① 从此组中删除计算机：只删除当前分组中的计算机，而不会影响到计算机在其他分组中的存在和应用。

② 将计算机移到此组的父组中：将组中的计算机移动到其父组中，由于当前组的父组是“所有计算机”，默认已经存在该计算机，所以不可操作。

③ 从此 WSUS 服务器中删除计算机：彻底删除本组的计算机，如果其他分组中也有该计算机则一同删除。

(2) 添加计算机

正确配置 WSUS 客户端后，服务器将自动发现这些客户机，并显示在“未分配的计算机”分组中，如图 6-27 所示。如果没有立即显示，可以尝试刷新一下服务器，或者在“状态”下拉列表框中选择适当的状态，如“任何”等。



图 6-27　发现的客户端计算机

如果接受管理的 WSUS 客户端数量较多，则可以通过“搜索”功能快速查找指定的计算机。右击“所有计算机”并选择快捷菜单中的“搜索”选项，打开如图 6-28 所示的“搜索”对话框。在“名称包含”文本框中输入客户端计算机的名称或计算机名中的部分字符，单击“立即查找”按钮，即可开始搜索。

在搜索结果中，右击希望添加或者管理的客户端，并选择快捷菜单中的“更改成员身份”选项，打开如图 6-29 所示的“设置计算机组成员身份”对话框，选择想要转移到的目标分组并单击“确定”按钮，即可将其添加到指定分组中。通过这种方法，可以快速管理多个名称类似的客户端计算机，在搜索结果中可以借助 Shift 键和 Ctrl 键同时选择多个客户端。

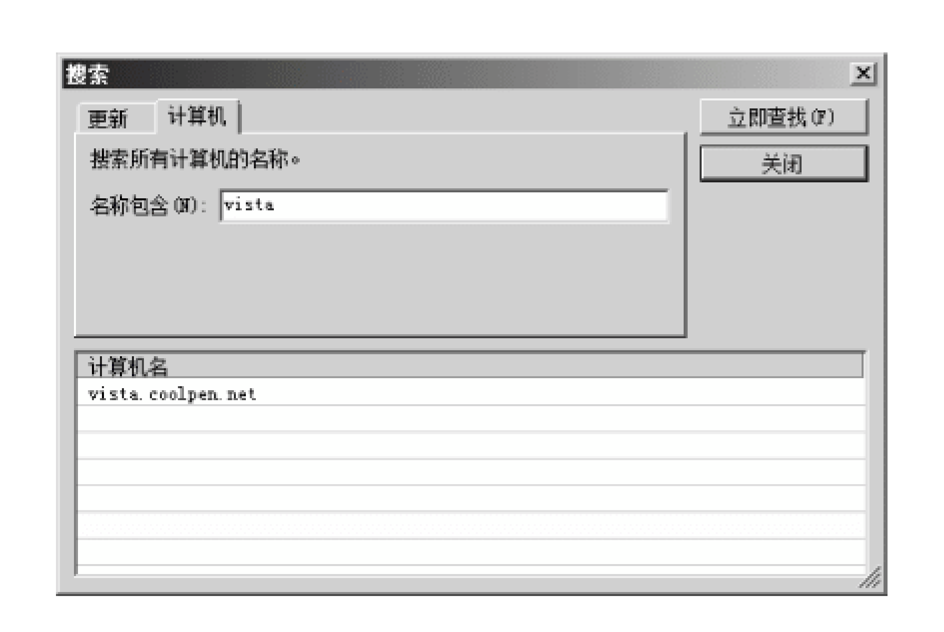



图 6-28 “搜索”对话框



图 6-29 “设置计算机组成员身份”对话框(1)

提示：如果使用客户端计算机上的组策略或注册表设置管理客户端，则无法完成此设置。

(3) 删除组中的计算机

如果管理员不希望将针对计算机组的设置，应用到其中的某台客户端上，此时应将其从组中删除。例如，现在需要删除 test 分组中的某一台计算机，可以在 Update Services 窗口中右击希望删除的计算机并选择快捷菜单中的“更改成员身份”选项，打开如图 6-30 所示的“设置计算机组成员身份”对话框，取消 test 分组即可。此时，只是将客户端从当前组(test 组)中删除，并被自动添加到“未分配的计算机”组中，但仍然接受 WSUS 服务器的管理。



图 6-30 “设置计算机组成员身份”对话框(2)

提示：如果使用客户端计算机上的组策略或注册表设置管理客户端，则无法完成此设置。

当分组中的某些客户端无须再从 WSUS 服务器获取更新，或者由于其他原因退出网络时，应及时在 WSUS 服务器上将其删除。展开所在分组并找到要删除的计算机名称，右击计算机名称并选择快捷菜单中的“删除”选项，提示“删除计算机”对话框，单击“是”按钮，即可将其从 WSUS 服务器中删除。

2. 监视 WSUS 服务器和客户端状况

WSUS 服务器还提供了报告监视功能，可以轻松实现对 WSUS 服务器运行情况，以及客户端安全状态的实时监控，也可以选择从当前服务器的下游服务器汇总数据，包括更新报告、计算机报告和同步报告 3 类。默认情况下，WSUS Reporters 安全组的成员具有运行和查看 WSUS 报告的权限，本地 Administrator 具有运行和查看 WSUS 报告的权限。

(1) 更新报告

更新报告包括如下 3 种。

① 更新状态摘要报告。该报告可以提供每个更新的详细摘要,其中包括更新属性和审批状态。生成此报告时,将会在树窗格中看到报告条件中包含的所有更新。

② 更新状态详细报告。该报告可以显示所有计算机中各个更新的状态。

③ 更新状态表格报告。该报告可以提供多个更新的更新状态。生成此报告时,将会在表中看到报告条件中包含的所有更新。

各种更新报告的查看,完全相同。以查看更新状态摘要报告为例,操作步骤如下。

① 在“报告”窗口中,单击“更新状态摘要报告”,打开如图 6-31 所示的“LXH 的更新报告”窗口。这里包括更新级别、所属产品类型、计算机分组、更新执行结果等设置选项,用户可以对希望查看的更新类型和级别进行选择。

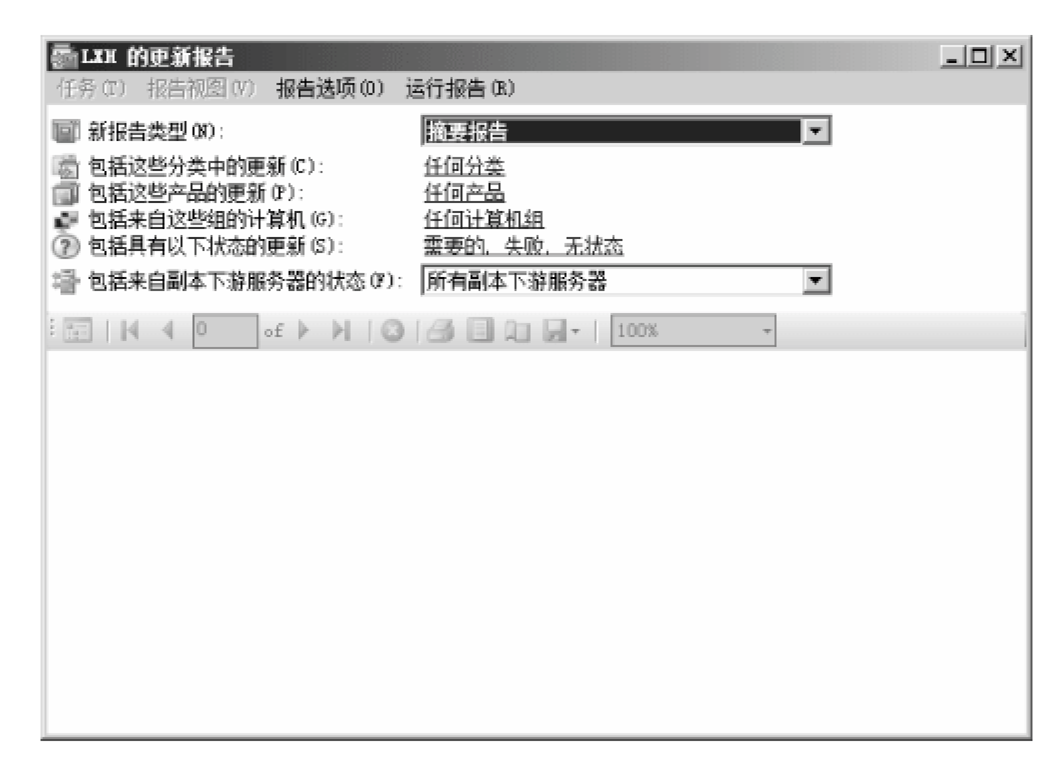


图 6-31　设置生成报告的更新属性

② 选择“运行报告”菜单选项,显示如图 6-32 所示的“更新状态摘要报告”窗口,根据所选更新的不同,生成报告所需的时间及内容也会有所不同,默认情况下,每页仅显示一项更新的相关信息,包括描述、分类、严重等级、编号以及审批情况等。



图 6-32　“更新状态摘要报告”窗口

③ 单击“导出”图标按钮,可以将当前报告信息导出到 Excel 电子表格或 PDF 格式的文件中。

(2) 计算机报告

计算机报告主要用于反映客户端系统更新状态和详细系统信息,管理员可以根据此结果了解当前网络安全状态,包括如下 3 种。

① 计算机状态摘要报告。该报告可以提供每台计算机的详细摘要，其中包括计算机组信息和更新安装状态。

② 计算机状态详细报告。该报告可以显示计算机状态摘要以及每个更新的状态。

③ 计算机状态表格报告。该报告可以提供多台计算机的计算机状态。生成此报告时，将会在表中看到报告条件中包含的所有计算机。

（3）同步报告

同步结果报告显示 WSUS 服务器的上次同步结果，或者显示特定时间段内的同步结果。在树窗格中，报告结果将作为摘要显示，并且还按更新分类进行分组。通过在树窗格中选择分类，用户将会在“同步报告”窗格中看到有关这些更新的同步状态的详细信息。

默认情况下，同步报告仅显示最近 30 天的同步结果，用户可以根据需要选择不同的时间段来筛选报告结果。在新的更新列表中单击特定更新，即可通过该报告查看有关该更新的详细信息。

3. 设置特殊文件发布

在应用 WSUS 发布补丁程序过程中，可能会遇到有些文件无法通过服务器发布给客户端的情况，例如.reg 格式的注册表文件等。这是因为在 WSUS 服务器使用的 Web 站点的 MIME 类型中没有定义该文件类型。为了顺利将更新文件发布到客户端，应先将对应文件类型添加到 IIS 全局或 WSUS 服务器对应站点的 MIME 类型库中，操作步骤如下（此处以向 WSUS 服务使用的站点中添加为例）。

（1）打开“Internet 信息服务(IIS)管理器”窗口，展开 WSUS 服务使用的 Web 站点，本例中为默认站点 Default Web Site，在 IIS 区域中找到“MIME 类型”，如图 6-33 所示。



图 6-33 IIS 管理器

（2）双击“MIME 类型”图标，打开如图 6-34 所示的“MIME 类型”窗口，这里显示了当前站点支持的所有 MIME 类型。

（3）单击“添加”按钮，显示如图 6-35 所示的“添加 MIME 类型”对话框。在“文件扩展



图 6-34 “MIME 类型”窗口

名”文本框中，输入想要添加的文件扩展名(如.reg)，并在“MIME 类型”文本框中，按照“类型\子类型”格式输入相应的类型。



图 6-35 “添加 MIME 类型”对话框

提示：用户可以使用通配符“ * ”同时添加多种 MIME 类型，例如在“文件扩展名”文本框中输入“. * ”，则允许发布任何类型的文件，此时可能会对服务器安全造成威胁，慎用此设置。

(4) 最后单击“确定”按钮保存设置即可。

6.3.4 知识链接：WSUS

1. WSUS 安装注意事项

WSUS 对服务器的要求不同，甚至在 Windows Vista 等客户端系统中都可以安装。因此，只要根据系统需求，准备好保存系统更新的 NTFS 分区即可。其他组件，如 IIS 等，在利用 Windows Server 2008 的“添加角色向导”安装 WSUS 时会自动安装，用户只需要在安装 WSUS 前安装 Microsoft Report Viewer 组件即可。

Microsoft Report Viewer 是使用 WSUS 3.0 SP2 用户界面的必备组件，用来查看 WSUS 更新或同步的各种报告。适用于 WSUS 3.0 SP2 的版本是 Microsoft Report Viewer 2008 SP1 Redistributable，可以从 Microsoft 网站下载，下载地址为：

http://www.microsoft.com/downloads/details.aspx?familyid=BB196D5D-76C2-4A0E-9458-267D22B6AAC6&displaylang=zh-cn

2. 自动审批

默认情况下，WSUS 服务器是不运行任何自动审批规则的，即完全由管理员手动审批完成。通过启用自动审批功能，可以将特定的分类和产品类型的更新，审批到指定的客户端，这样可以大大减轻管理员的工作负担，但仅限于可靠性较高的更新。为避免安装更新之后可能导致的各种麻烦，建议审批之前进行严格测试，确认无误后再审批到客户端。

6.4 Windows 客户端配置

凡是具备自动更新功能的 Windows 操作系统，都可以配置为 WSUS 客户端。根据客户端计算机所在网络环境的不同，可以采取不同的配置方法。在域环境中，可以使用组策略对象(GPO)完成；在工作组环境中，可以使用本地组策略对象或者直接修改注册表完成。需要注意的是，将计算机配置为 WSUS 客户端后，客户端计算机“控制面板”中的自动更新就会失效。

6.4.1 通过组策略编辑器配置

如果通过组策略为 Active Directory 网络中的计算机指定 WSUS 升级服务器的地址，需要在包括网络中所有计算机的“组织单元”或其上一级“组织单元”配置组策略，或者将需要更新的计算机“移动”到一个新创建的“组织单元”中，然后再对该组中的所有计算机进行操作。

(1) 新建一个用于保存所有 WSUS 客户端计算机的组织单位，当然也可以使用 Active Directory 默认提供的组织单位。使用新建计算机的方法将客户端计算机添加到指定的组织单位中，也可以从其他组织单位中直接拖曳。

(2) 依次选择“开始”→“管理工具”→“组策略管理”选项，打开“组策略管理”窗口，依次展开“林”→“域”→coolpen. net→test(新建的组织单位)选项。右击 test 并选择快捷菜单中的“在这个域中创建 GPO 并在此处链接”选项，打开如图 6-36 所示的“新建 GPO”对话框，在“名称”文本框中，输入便于识别的名称。



图 6-36 “新建 GPO”对话框

(3) 右击新建的 GPO 并选择快捷菜单中的“编辑”选项，打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→Windows Update 选项。双击“配置自动更新”选项，打开如图 6-37 所示的“配置自动更新 属性”对话框，先选中“已启用”单选按钮激活下面的选项，然后在“配置自动更新”右侧的下拉列表框中选择对应的自动更新类型，有 2～5 共 4 种类型，当选择第 4 种类型“自动下载并计划安装”，即自动

下载更新并计划安装时还要继续设置“计划安装日期”和“计划安装时间”选项，指定执行安装的时间和日期。设置完成后单击“应用”和“确定”按钮，保存设置。

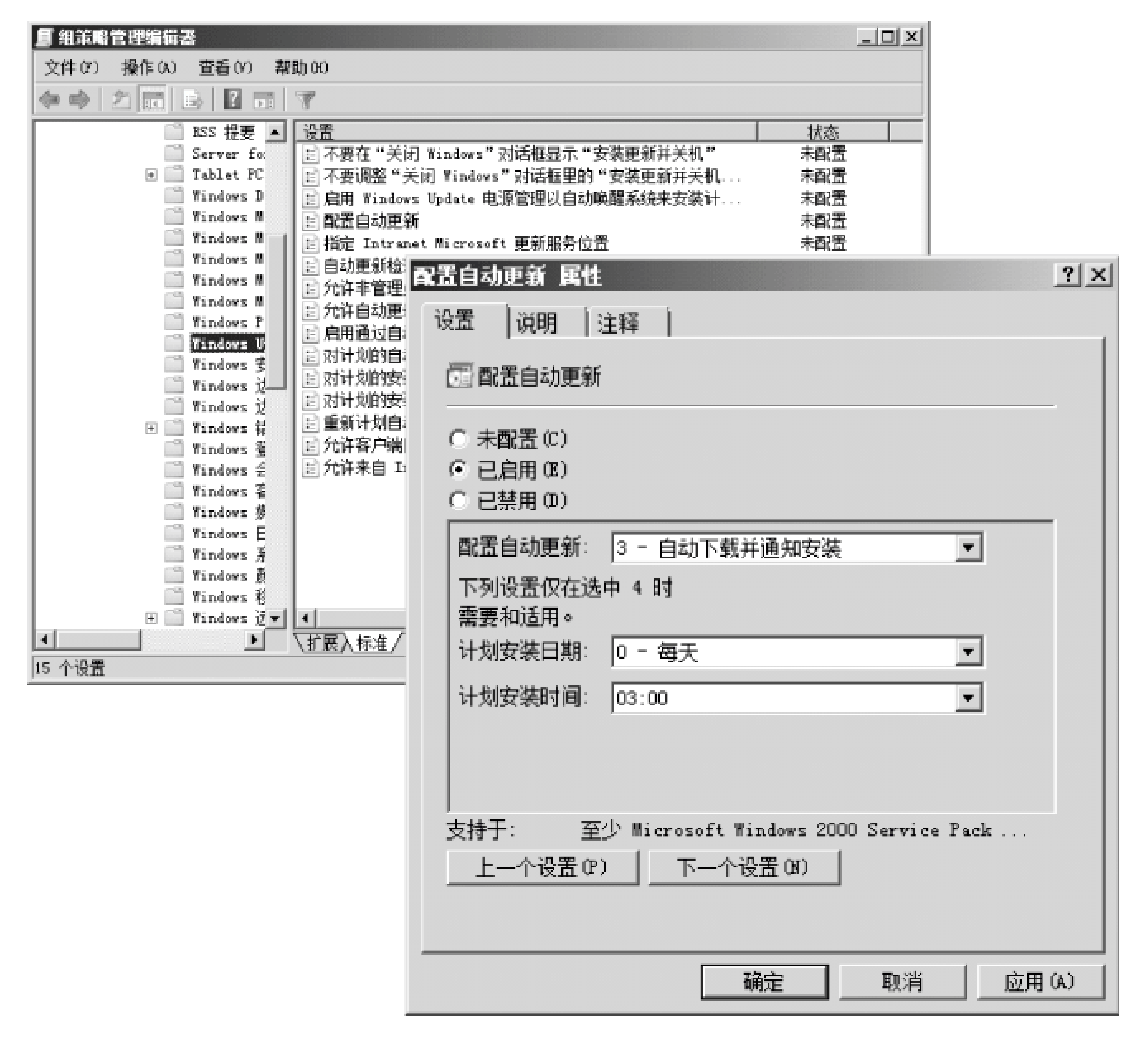


图 6-37 启用自动更新功能

(4) 双击“指定 Intranet Microsoft 更新服务位置”策略，打开如图 6-38 所示的“指定 Intranet Microsoft 更新服务位置 属性”对话框。首先选中“已启用”单选按钮，然后在“设置检测更新的 Intranet 更新服务”文本框中，指定局域网中的 WSUS 服务器地址，在“设置 Intranet 统计服务器”文本框中，指定用于获取客户端状态信息的服务器地址，本例中使用的是一台服务器。如果网络中的 WSUS 服务器和统计报表服务器(只用于获取客户端的状态和需求信息)分别是不同的服务器，则此处指定时应格外注意。

注意：设置这两条策略的顺序千万不可颠倒，否则将不会生效，即必须先启用“配置自动更新”，然后才可以设置 WSUS 服务器地址。

(5) 保存组策略编辑结果即可。其他组策略现象用户也可以根据自己的需要进行修改，此处不再详细介绍。

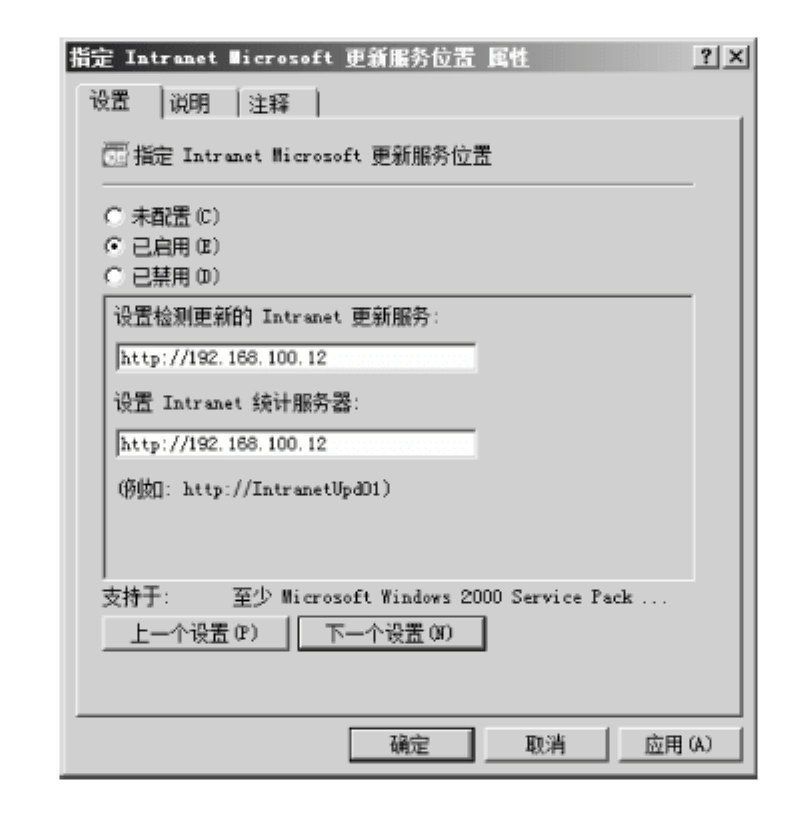


图 6-38 “指定 Intranet Microsoft 更新服务位置 属性”对话框

6.4.2 通过本地策略配置

通过组策略或本地策略编辑器配置 WSUS 客户端，是常用的方法之一。对于域环境中的计算机，则管理员可以在域控制器上创建应用于需要配置客户端的组策略，并进行相应编

辑；而工作组中的计算机则可以通过修改本地策略使其成为 WSUS 客户端。此处，以工作组环境中的 Windows Vista 客户端为例加以介绍。

(1) 以管理员账户登录计算机，在“组策略对象编辑器”窗口中，依次展开“计算机配置”→“管理模板”→“Windows 组件”→Windows Update 选项，如图 6-39 所示。与配置域组策略完全相同，需要依次配置“配置自动更新”和“指定 Intranet Microsoft 更新服务位置”策略，配置过程此处不再赘述。

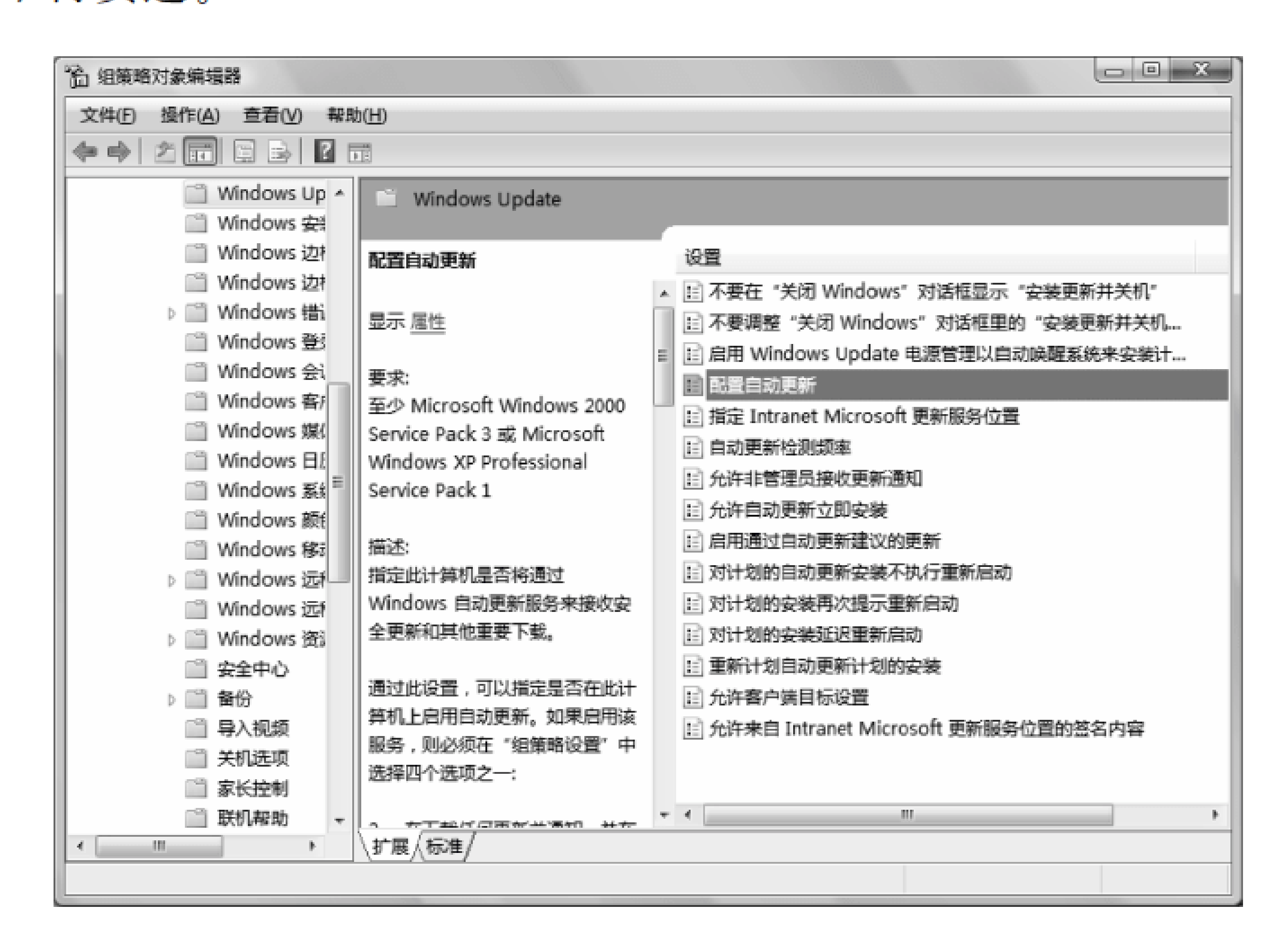
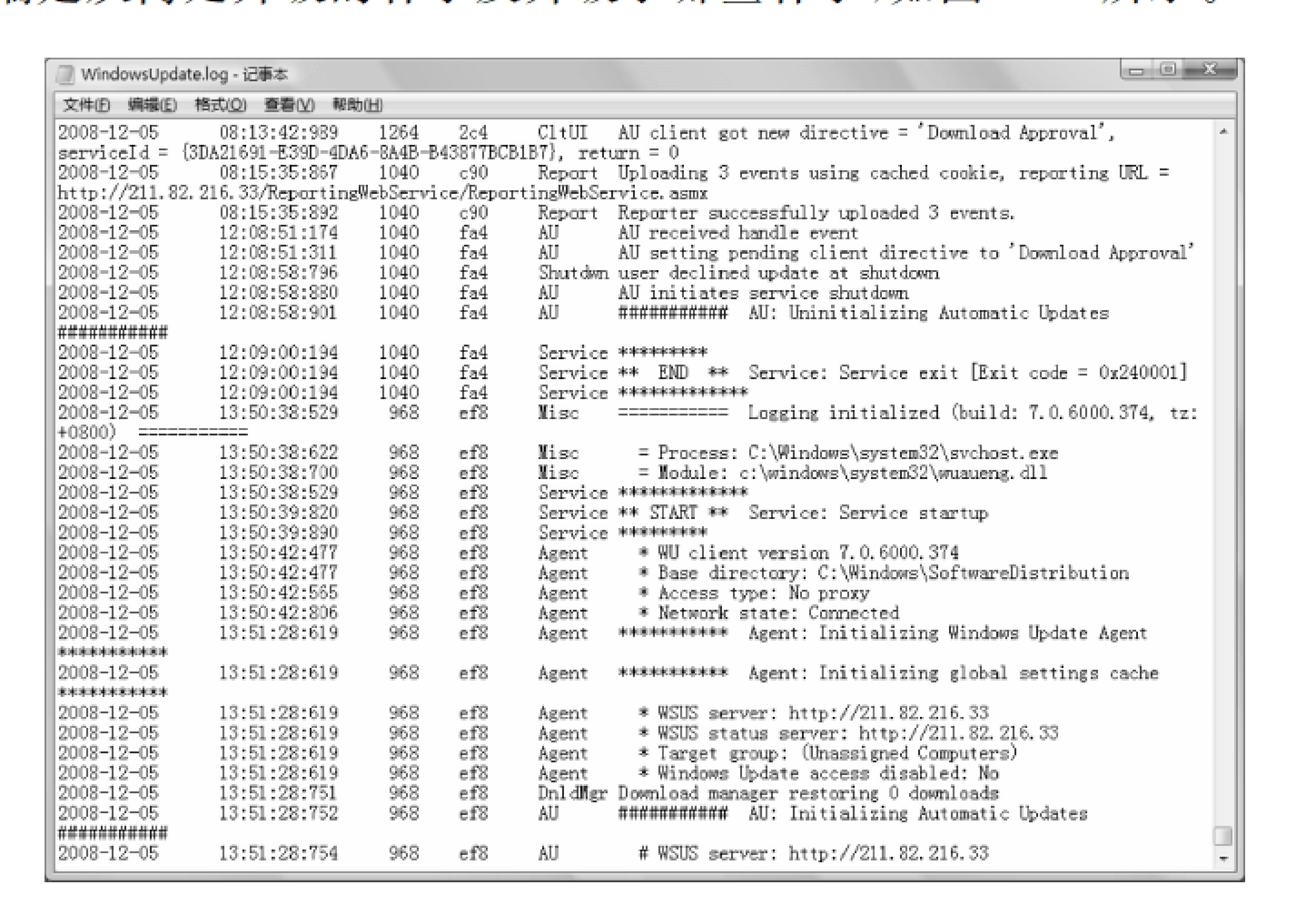


图 6-39 “组策略对象编辑器”窗口

(2) 配置完 WSUS 客户端后，在 Windows 目录下会生成 WindowsUpdate.log 文件，可以查看此客户端是从何处升级的补丁及升级了哪些补丁，如图 6-40 所示。


WindowsUpdate.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
2008-12-05	08:13:42:989	1264	2c4	CltUI	AU client got new directive = 'Download Approval', serviceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}, return = 0
2008-12-05	08:15:35:867	1040	c90	Report	Uploading 3 events using cached cookie, reporting URL = http://211.82.216.33/ReportingWebService/ReportingWebService.asmx
2008-12-05	08:15:35:892	1040	c90	Report	Reporter successfully uploaded 3 events.
2008-12-05	12:08:51:174	1040	fa4	AU	AU received handle event
2008-12-05	12:08:51:311	1040	fa4	AU	AU setting pending client directive to 'Download Approval'
2008-12-05	12:08:58:796	1040	fa4	Shutdwn	user declined update at shutdown
2008-12-05	12:08:58:880	1040	fa4	AU	AU initiates service shutdown
2008-12-05	12:08:58:901	1040	fa4	AU	###########  AU: Uninitializing Automatic Updates ###########
2008-12-05	12:09:00:194	1040	fa4	Service	*********
2008-12-05	12:09:00:194	1040	fa4	Service	**  END  **  Service: Service exit [Exit code = 0x240001]
2008-12-05	12:09:00:194	1040	fa4	Service	*************
2008-12-05	13:50:38:529	968	ef8	Misc	===========  Logging initialized (build: 7.0.6000.374, tz: +0800)  ===========
2008-12-05	13:50:38:622	968	ef8	Misc	  = Process: C:\Windows\system32\svchost.exe
2008-12-05	13:50:38:700	968	ef8	Misc	  = Module: c:\windows\system32\wuaueng.dll
2008-12-05	13:50:38:529	968	ef8	Service	*************
2008-12-05	13:50:39:820	968	ef8	Service	** START **  Service: Service startup
2008-12-05	13:50:39:890	968	ef8	Service	*********
2008-12-05	13:50:42:477	968	ef8	Agent	  * WU client version 7.0.6000.374
2008-12-05	13:50:42:477	968	ef8	Agent	  * Base directory: C:\Windows\SoftwareDistribution
2008-12-05	13:50:42:565	968	ef8	Agent	  * Access type: No proxy
2008-12-05	13:50:42:806	968	ef8	Agent	  * Network state: Connected
2008-12-05	13:51:28:619	968	ef8	Agent	***********  Agent: Initializing Windows Update Agent ***********
2008-12-05	13:51:28:619	968	ef8	Agent	***********  Agent: Initializing global settings cache ***********
2008-12-05	13:51:28:619	968	ef8	Agent	  * WSUS server: http://211.82.216.33
2008-12-05	13:51:28:619	968	ef8	Agent	  * WSUS status server: http://211.82.216.33
2008-12-05	13:51:28:619	968	ef8	Agent	  * Target group: (Unassigned Computers)
2008-12-05	13:51:28:619	968	ef8	Agent	  * Windows Update access disabled: No
2008-12-05	13:51:28:751	968	ef8	DnldMgr	Download manager restoring 0 downloads
2008-12-05	13:51:28:752	968	ef8	AU	###########  AU: Initializing Automatic Updates ###########
2008-12-05	13:51:28:754	968	ef8	AU	  # WSUS server: http://211.82.216.33
```

图 6-40 WSUS 客户端更新日志

提示：对于单独客户端而言，至此 WSUS 客户端配置已经完成。但是如果需要在其他同配置计算机上部署 WSUS 客户端，逐一配置不仅浪费时间，而且容易出错。此时，可以按照如下步骤导出相关键值，然后在需要部署的计算机上重新导入即可。

(3) 打开“注册表编辑器”窗口，依次展开 HKEY_LOCAL_MACHINE→SOFTWARE→Policies→Microsoft→Windows→WindowsUpdate 选项，右击 WindowsUpdate 并选择快捷菜单中的“导出”选项，将其保存到本地计算机上，如图 6-41 所示。

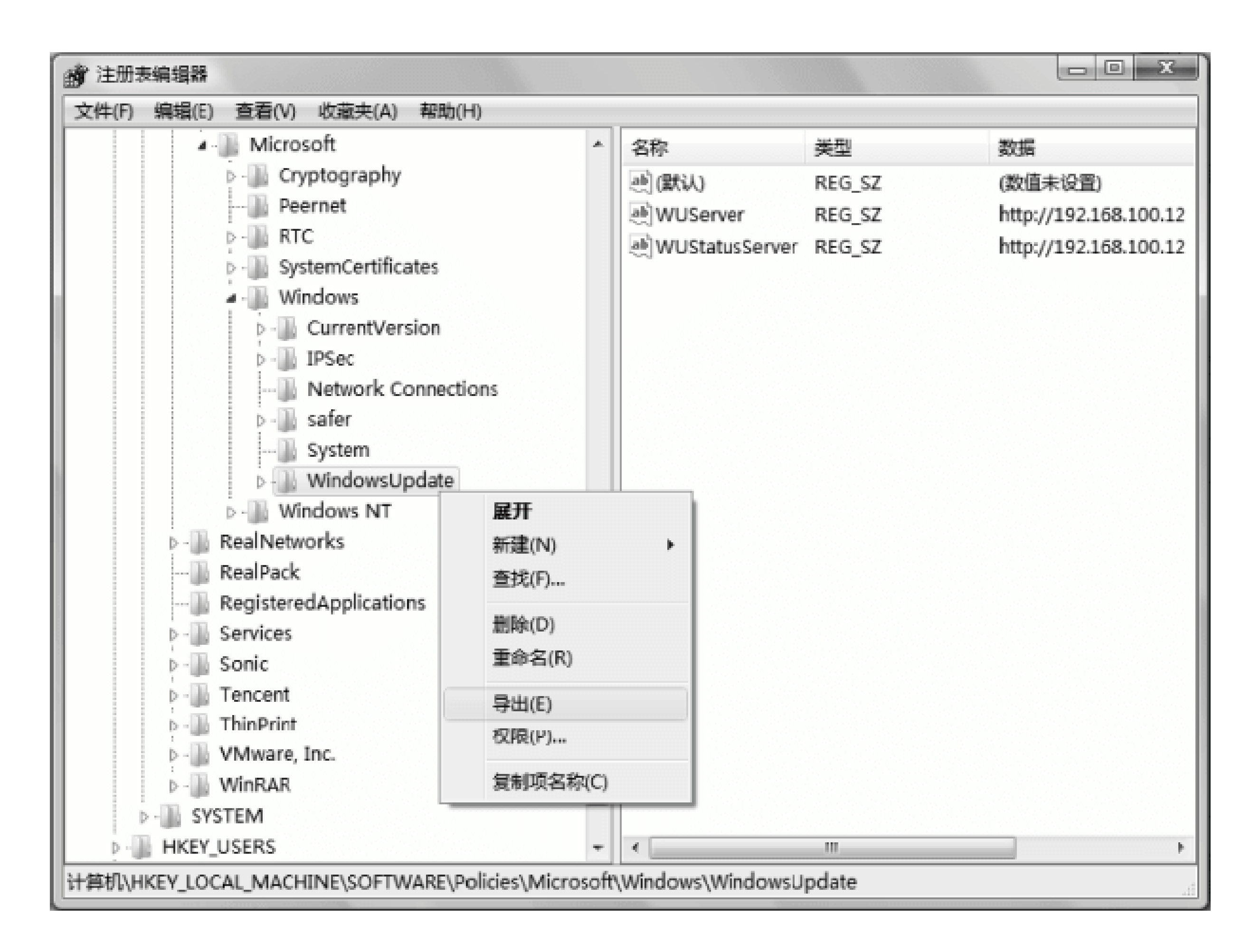


图 6-41 导出注册表键值

(4) 在其他需要部署 WSUS 客户端的计算机上，双击运行导出的注册表文件，显示“注册表编辑器”对话框，单击“是”按钮即可将其包含的项和值成功添加到注册表中。

提示： *右击导出的注册表文件，并选择“编辑”选项，即可查看其中的具体内容，全文如下。如果 WSUS 服务器地址或端口发生变化，只需重新修改注册表文件中的相关字段，保存之后，再次导入即可，非常方便。*

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"="http://192.168.100.12"
"WUStatusServer"="http://192.168.100.12"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000002
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"UseWUServer"=dword:00000001
```

6.4.3 客户端获取并安装更新

WSUS 客户端获取的更新的操作都是“被动”的，即只能接受 WSUS 服务器的管理和控制，当服务器发布了适用于当前客户端系统的更新之后，系统任务栏中将显示相关提示信息，询问用户是否下载或安装，方法与使用 WSUS 服务器之前完全相同，此处不再赘述。

6.4.4 知识链接：组策略

由于组策略的刷新和应用需要一定的时间，所以保存编辑结果后，即使客户端重新登录

了域控制器也可能无法立即联系到 WSUS 服务器。而默认情况下，每隔 90min 计算机组策略便会在后台刷新一次，刷新的时间可能随机偏移 0～30min，客户端计算机要在域控制器刷新组策略 20min 后才可以应用到组策略。如果想要以更快的速度刷新组策略，可以在服务器端设置组策略后，通过运行 gpupdate 命令让设置即时生效，并在客户端计算机通过运行 gpupdate /force 命令立刻生效。如果计算机不是 Active Directory 的成员，可以通过运行 wuauclt. exe /detectnow 命令来消除 20min 的延时。

习题

1. 简述企业网络中 WSUS 服务器是如何运作的及有哪些优点。
2. WSUS 服务器的数据库中包含哪些信息？
3. 如何配置 WSUS 服务器为客户端自动审批更新？

实验：通过各种方式部署 WSUS 客户端

实验目的：

能够应用企业网络中的 WSUS 服务器实现 Windows Update。

实验内容：

运用各种方式将客户端计算机配置为 WSUS 客户端，例如组策略、本地策略、导入注册表文件等。

实验步骤：

(1) 在域中部署备用的 WSUS 服务器。
(2) 在客户端计算机上运行 ping 命令，分别测试到 WSUS 服务器的连通性。
(3) 使用组策略方式为域中的指定计算机启用 WSUS 客户端。
(4) 登录工作组中的计算机，通过修改本地组策略启用 WSUS 客户端。
(5) 通过导入注册表文件，快速配置 WSUS 客户端。
(6) 测试 WSUS 客户端是否能通过 WSUS 服务器获取系统更新。

第 7 章 chapter 7

Cisco IOS安全

路由器和交换机是计算机网络中应用最多的网络设备,其安全性直接影响到整个网络的可用性和稳定性,对于网络安全起着至关重要的作用。目前,大多数网络设备都是可网管的,即拥有独立的操作系统,允许管理员进行各项应用配置和安全配置。常见的基于 Cisco IOS 的安全配置包括设置密码、关闭多余服务、启用加密传输等。

7.1 Cisco IOS 安全规划

在网络安全方面,Cisco 公司提供了专业的网络安全防御设备,例如网络防火墙、入侵检测系统、入侵防御系统等,并且大部分网络设备均支持一定的网络安全配置功能。不仅如此,Cisco 还允许用户通过配置 IOS 安全功能,来部署更为严密的安全防护。IOS 安全体系结构已经经过 10 多年的技术革新发展历程,能够为企业的安全防御提供坚实基础。

7.1.1 案例情景

目前该企业网络中,大部分网络设备均为 Cisco 系列的可网管系列产品。安全配置与访问效率本来就是相互矛盾的,过多的安全验证措施势必会影响网络访问和传输速率。为了加快访问和传输速率,不进行任何安全配置是非常危险的。目前,该网络中只有基于物理设备的安全防护,基于网络设备 IOS 的安全配置非常有限,存在严重的安全隐患。网络安全仍有较大的提升空间。

7.1.2 项目需求

一方面是访问和工作效率;另一方面是网络安全。对于企业而言,必须决定何时在用户的访问和工作效率与可能被用户视为限制的安全措施之间进行折中,寻求两者之间的平衡,才是最完美的解决方案。因此,应注重一些合理安全措施的广泛部署,例如加密,对网络用户的影响较小,又可以大大提升网络安全性。

严格限制管理员的访问权限,不仅需要为管理员账户设置登录密码,而且应为不同用户配置不同的管理员账户,并赋予不同的操作权限级别。目前,该网络中并没有详细的 VLAN 划分,因此网络访问比较混乱,网络设备工作效率不高,需要根据用户部门或职能的不同进行合理的 VLAN 划分,限制用户之间的相互访问,尤其是安全性要求较高的 VLAN 更应严格限制网络通信。

7.1.3 解决方案

基于 Cisco IOS 的安全配置管理主要包括访问管理、宿主安全、传输加密、传输控制、VLAN 划分、日志收集与分析、访问控制列表等。鉴于该网络当前的安全需求，可以从如下几个方面配置网络安全。

(1) 访问管理。访问管理控制方法、方案以及网络资源的发布，并提供监督和控制。目前，企业网络安全正面临管理主机和网络设备以及远程计算机的挑战，关键是给网络管理员提供控制访问的多种方法。访问管理是 Cisco IOS 安全体系的重要方面。为了满足大量用户的访问需求，Cisco IOS 安全体系为客户端提供广泛的访问管理功能。

(2) Cisco IOS 特权级别。每个用户都拥有独特的访问管理要求。系统管理员可以通过定制对 IOS 软件用户界面的访问，从而使他们能够建立对网络设备和服务器的访问特权级别。用户可以建立多达 16 个访问级别。融合多个特权级别可以实现更加精细的访问层次，对于 Cisco IOS 用户界面的每一级而言，都可以建立单独的加密口令。

(3) 访问控制列表。访问控制列表的主要功能是提供数据包过滤。通过在核心交换机或路由器上配置访问控制列表，可以自动过滤掉某些类型的网络访问，即可节约网络设备的开销，又可以提升网络安全性。

(4) 划分 VLAN。在汇聚层交换机上划分 VLAN，将所有客户端分配到不同的 VLAN 中，既可隔离网络广播提高通信速率，又可以确保机密信息的安全，控制客户端之间的网络访问。

(5) 身份验证。启用网络设备的身份验证功能，对接入网络的设备或用户进行严格身份验证，尤其是在无线网络中，可以通过加密传输、禁止广播 SSID 和身份验证等多项安全措施，确保网络安全。

7.2 Cisco IOS 系统安全

IOS(Internet Operation System Software，网际操作系统)是 Cisco 公司跨越主要路由和交换产品的软件平台，类似于计算机的操作系统，也是由软件工程师编写而成的，难免会存在系统漏洞，而针对网络设备的攻击利用的就是 IOS 自身的漏洞。影响网络设备 IOS 安全的因素是多方面的，例如登录密码安全、SNMP 安全、系统安全日志等。

7.2.1 登录密码安全

Cisco 的 Enable 密码与 Windows 的 Administrator 密码的作用和重要性完全相同。只要知道了 Enable 密码，就可以对交换机进行任意配置和管理。

1. 配置 Enable 密码

默认状态下，Cisco 设备的 Enable 密码为空，所以，在对交换机进行初始配置时，必须为其设置 Enable 密码。Enable 密码配置过程如下。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 为特权模式指定新的 Enable 密码。Enable 密码可包括 1～25 个大写和/或小写字母,也可以包括数字。密码长度应当大于 6 个字符,并且应当是包含大小写字母和数字的无意义的字符串。访问级别(level)可取值范围为 0～15,级别 1(Level 1)是 normal user EXEC 模式,拥有最低权限。级别 15 是 privileged EXEC 模式,拥有最高权限,默认级别是 15。

```
Cisco(config)# enable secret[level level]password
```

或

```
Cisco(config)# enable password[level level]password
```

提示: 密码的第 1 个字符不能是数字。当有多个网络管理员时,可以为不同的级别分别设置不同的访问密码。这样,既可以让他们查看网络配置,诊断网络故障,同时,又可以保障网络设备的配置安全。

(3) 加密新的密码。

```
Cisco(config)# service password-encryption
```

(4) 返回特权模式。

```
Cisco(config)# end
```

(5) 保存修改后的配置。

```
Cisco# copy running-config startup-config
```

2. 配置 Telnet 密码

Telnet 密码配置过程如下。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 输入 Telnet 进程号,进入 Line 配置模式。在一台交换机和路由器上,最多可以实现 16 个 Telnet 进程,方便多个用户同时查看和管理。"0 15"表明配置所有的可能的 16 个进程。

```
Cisco(config)# line vty 0 15
```

(3) 指定 Telnet 密码。Telnet 密码设置要求与 Enable 相同。

```
Cisco(config)# password password
```

(4) 返回特权模式。

```
Cisco(config)# end
```

(5) 保存修改后的配置。

```
Cisco# copy running-config startup-config
```

3. 配置管理用户

管理用户配置过程如下。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 设置管理用户,并为其指定级别。用户名中间不能有空格和引号。级别(Level)可取值范围为0～15,15拥有特权模式访问权限,而0只拥有普通用户权限。用户密码(Password)设置要求与Enable密码相同。

```
Cisco(config)# username name[privilege level]{password password}
```

(3) 进入Line配置模式,配置Console(Line 0)或VTY Line(Line 0～15)。

```
Cisco(config)# line console 0
```

或

```
Cisco(config)# line vty 0 15
```

(4) 用户登录到设备时,启用本地密码检查。

```
Cisco(config-line)# login local
```

(5) 返回特权模式。

```
Cisco(config)# end
```

(6) 保存修改后的配置。

```
Cisco# copy running-config startup-config
```

7.2.2 配置命令级别安全

控制网络上的终端访问交换机的一个简单办法,是使用密码保护和划分特权级别。密码可以控制对网络设备的访问,特权级别可以在用户登录成功后,控制其可以使用的命令。

1. 配置多个用户级别

为某个配置命令设置多个用户级别时,配置过程如下。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 设置命令的级别划分。mode用于指定命令的模式。其中,configure表示全局配置模式,exec表示特权命令模式,interface表示接口配置模式,line表示Line配置模式。level用于授权级别,范围从0～15。level 1是普通用户级别,level 15是特权用户级别,在各用户级别间切换可以使用enable命令。command则用于指定欲授权的命令。

```
Cisco(config)# privilege mode level level command
```

提示: 当将一条命令的权限授予某个级别时,则该命令的所有参数和子命令都同时被授予该级别,除非该授权被收回。

(3) 返回特权模式。

```
Cisco(config)# end
```

（4）保存修改后的配置。

```
Cisco# copy running-config startup-config
```

若欲恢复一条已知的命令授权，可以在全局配置模式下使用 no privilege mode level level command 命令。

2. 登录和离开授权级别

在特权命令模式下，可以登录到指定的授权级别，或者离开某个授权级别。

登录到指定的授权级别。level 用于指定级别，范围从 0～15。

```
Cisco# enable level
```

离开到指定的授权级别。

```
Cisco# disable level
```

7.2.3 终端访问限制安全

通过限制对交换机、路由器等网络设备的访问，可以最大限度地避免可能的来自内部或外部的恶意网络攻击，并可有效地预防未授权用户或权限较低的网络管理员修改网络配置，从而保护网络传输的稳定和安全。

1. 控制虚拟终端访问

控制虚拟终端访问配置过程如下。

（1）进入全局配置模式。

```
Cisco# configure terminal
```

（2）配置 IP 访问列表。

```
Cisco(config)# access-list access-lis-number permit ip-address
```

提示：Cisco 交换机的访问列表配置与 Cisco 路由器完全相同，详细操作参考本章“路由器 IOS 安全配置”中的相关内容。

（3）进入 Line 配置模式。

```
Cisco(config)# line vty 0 4
```

（4）启用 IP 访问列表。

```
Switch(config-line)# access-class access-class-number in
```

（5）返回特权模式。

```
Cisco(config-line)# end
```

（6）保存修改后的配置。

```
Cisco# copy running-config startup-config
```

2. 控制会话超时

具体更改超时时间的操作步骤如下。

（1）进入全局配置模式。

```
Cisco# configure terminal
```

（2）进入 Line 配置模式。

```
Cisco(config)# line vty 0 4
```

（3）设置超时连接的时间。取值范围为 0～35791，建议采用 180。

```
Switch(config-line)# exec-timeout seconds
```

（4）返回特权模式。

```
Cisco(config-line)# end
```

（5）保存修改后的配置。

```
Cisco# copy running-config startup-config
```

7.2.4 SNMP 安全

SNMP 字符串的作用类似于密码，允许拥有合法认证名的用户同交换机上的代理通信。因此，需要对 SNMP 字符串的安全进行重点保护。

1. 配置 SNMP 字符串

为了更加安全地使用 SNMP，可以指定以下一个或者几个属性同认证名绑定。

① IP 地址，通过指定 IP 地址，只允许该 IP 地址的管理者有权同代理通信。

② 读写权限，通过指定读写权限，限制管理者的操作。

（1）进入全局配置模式。

```
Cisco# configure terminal
```

（2）设置 SNMP 字符串。string 用于定义字符串，应当使用较长的、没有意义的、不容易被猜到的字符。ro 表示定义只读字符串，只享有配置读取权限；rw 表示可写字符串，享有配置修改权限。access-list-number 用于指定 IP 标准访问列表号，取值范围为 1～99 和 1300～1999。

```
Cisco(config)# snmp-server community string[ro|rw][access-list-number]
```

（3）如果在上面指定了 IP 访问列表，那么，就应当在这里进行创建。需要时，可以重复执行该命令，以创建多条访问列表项。access-list-number 应当与上述所引用的访问列表号相同。deny 关键字将禁止与之匹配的访问，permit 关键字则允许与之匹配的访问。source 用于指定 SNMP 管理的 IP 地址。source-wildcard（可选）用于指定 IP 地址范围的反码。从安全的角度考虑，只需设置 permit 允许特定 IP 地址即可。

```
Cisco(config)# access-list access-list-number{deny|permit}source[source-wildcard]
```

（4）返回特权模式。

```
Cisco(config)# end
```

（5）保存修改后的配置。

```
Cisco# copy running-config startup-config
```

2. 配置 SNMP 组和用户

（1）进入全局配置模式。

```
Cisco# configure terminal
```

（2）为每个本地或远程 SNMP 复制配置名称。engineid-string 是一个 24 字符的 SNMP 复制 ID 字符串，不过，为 0 的部分不需要输入。例如，当欲配置的本地设备的引擎 ID 为 123400000000000000000000 时，只需输入 snmp-server engineID local 1234 即可。如果选择的是远程设备，那么，应当指定其 SNMP 复制的 IP 地址和 UDP 端口号即可。默认端口号为 162。

```
Cisco(config)# snmp-server engineID {local engineid-string | remote ip-address [udp-port port-number] engineid-string}
```

（3）在远程设备上配置新 SNMP 组。groupname 用于指定组名称。v1、v2c 和 v3 用于指定安全模式，其中，v1 安全模式最低，v3 安全模式最高。auth 用于启用 Message Digest 5（MD5）和 Secure Hash Algorithm（SHA）包认证。priv 用于启用 Enables Data Encryption Standard（DES）加密。noauthet 用于启用 noAuthNoPriv 加密级别。

```
Cisco(config)# snmp-server group groupname{v1|v2c|v3 {auth|noauth|priv}}[read readview][write writeview][notify notifyview][access access-list]
```

（4）为 SNMP 组添加新用户。username 用于指定该主机上的用户名称，groupname 用于指定将该用户加入的用户组。remote 用于指定用户所属的远程 SNMP 条目，其中，host 用于指定其主机名和 IP 地址，udp-port 用于指定端口号（默认值为 162）。v1、v2c、v3 用于指定 SNMP 版本。access-list 用于指定访问列表。如果指定为 v3，还需要指定相应的认证方式。

```
Cisco(config)# snmp-server user username groupname{remote host[udp-port port]}{v1[access access-list] | v2c [access access-list] | v3 [encrypted] [access access-list] [auth {md5 | sha} auth-password]}
```

（5）返回特权模式。

```
Cisco(config)# end
```

（6）保存修改后的配置。

```
Cisco# copy running-config startup-config
```

7.2.5 HTTP 服务安全

Cisco IOS 允许通过 Web 浏览器管理交换机和路由器，所需的 HTTP/HTTPS 服务器软件可在 IOS 11.0 及以后的版本中找到。这虽然使网络配置变得更加简单，但也可能由此而产生安全漏洞。因此，如非特别需要，建议关闭 HTTP/HTTPS 服务。

1. 关闭 HTTP 服务

若欲关闭 HTTP 服务,可依次运行如下命令。

```
Cisco# configure terminal
Cisco(config)# no ip http server
Cisco(config)# end
Cisco# copy running-config startup-config
```

使用 show running-config 命令进行查看时,会发现 HTTP 服务已经被关闭。若需启用 HTTP 访问,则输入下述命令。

```
Cisco# configure terminal
Cisco(config)# ip http server
Cisco(config)# end
Cisco# copy running-config startup-config
```

然后,再通过访问控制列表过滤允许访问网络设备的计算机。

2. 配置安全 HTTP 服务

交换机和路由器不但可以启用 HTTP 服务,还可以根据需要启用安全 HTTP 服务,让交换机和路由器作为认证服务器,从而提高网络传输的安全性。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 启用安全 HTTPS 服务。默认状态下,HTTPS 服务是被禁用的。

```
Cisco(config)# ip http secure-server
```

(3) (可选)指定 HTTPS 服务的端口号。默认端口号为 443,有效取值范围为 1025~65535。建议采用系统默认值 443。

```
Cisco(config)# ip http secure-port port-number
```

(4) (可选)为 HTTPS 连接指定 CipherSuites 加密算法。如果不指定加密算法,HTTPS 服务器与客户端将协商所采用的算法。默认为不指定加密算法。

```
Cisco(config)# ip http secure-ciphersuite{[3des-ede-cbc-sha][rc4-128-md5][rc4-128-sha][des-cbc-sha]}
```

(5) (可选)在连接处理期间,配置 HTTP 服务从客户端请求 X.509v3 证书。默认情况下,客户端将从服务器请求证书,但是,服务器不会尝试从客户端获取证书。

```
Cisco(config)# ip http secure-client-auth
```

(6) 指定 CA 信任点(Trustpoint)使用得到的 X.509v3 证书认证客户端连接。

```
Cisco(config)# ip http secure-trustpoint name
```

(7) (可选)为 HTTP 服务指定主目录。该路径通常位于网络设备本地的 Flash 闪存中。

```
Cisco(config)# ip http path path-name
```

(8)(可选)指定一个允许访问 HTTP 服务的访问列表。

```
Cisco(config)# ip http access-class access-list-number
```

(9)(可选)设置访问 HTTP 服务的并发最大数。取值范围为 1～16,默认值为 5。如果网络内只有一个网络管理员,那么,该值可以设置为 1。

```
Cisco(config)# ip http max-connections value
```

(10)(可选)指定在几种情形下,能够与 HTTP 服务保持多长时间的连接。idle 用于指定在没有数据发送和接收时所允许连接的最长时间,取值范围为 1～600s,默认值为 180s。life 用于指定所允许的连接持续的最长时间,取值范围为 1～86400s,默认值为 180s。requests 用于指定在一个连接上所允许的请求处理最大数,最大值为 86400,默认值为 1。从安全的角度考虑,idle 取值应当在 120～180s,life 取值应当在 180～300s,requests 取值为 1。

```
Cisco(config)# ip http timeout-policy idle seconds life seconds requests value
```

(11) 返回特权模式。

```
Cisco(config)# end
```

(12) 保存修改后的配置。

```
Cisco# copy running-config startup-config
```

3. 配置安全 HTTP 客户端

如果没有配置 CA 信任点,当远程 HTTPS 服务器请求客户端认证时,到该 HTTP 客户端的连接将失败。因此,必须配置安全 HTTP 客户端。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2)(可选)指定远程 HTTP 服务器请求客户端认证时使用的 CA 信任点。使用该命令的前提是已经配置了 CA 信任点。当然,如果客户端无须认证,或者根信任点已经存在,那么,该命令并非必需。

```
Cisco(config)# ip http client secure-trustpoint name
```

(3)(可选)为 HTTPS 连接指定 CipherSuites 加密算法。如果不指定加密算法,HTTPS 服务器与客户端将协商所采用的算法。默认为不指定加密算法。

```
Cisco(config)# ip http secure-ciphersuite{[3des-ede-cbc-sha][rc4-128-md5][rc4-128-sha][des-cbc-sha]}
```

(4) 返回特权模式。

```
Cisco(config)# end
```

(5) 保存修改后的配置。

```
Cisco# copy running-config startup-config
```

7.2.6 系统安全日志

网络设备的 Syslog 日志功能可以将某些重要事件信息(如系统错误、系统配置、状态变化、状态定期报告和系统退出等)或用户设定的期望信息传送给日志服务器,网络管理人员依据这些信息掌握设备的运行状况,及早发现问题,及时进行配置设定和排障,保障网络安全稳定的运行。

1. 启用系统日志信息

当系统日志信息被关闭后,借助以下操作,可以重新启用日志信息。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 启用系统日志信息。

```
Cisco(config)# logging on
```

(3) 返回特权模式。

```
Cisco(config)# end
```

(4) 查看日志信息状态。

```
Cisco# show running-config
Cisco# show logging
```

(5) 保存修改后的配置。

```
Cisco# copy running-config startup-config
```

2. 设置日志信息目的设备

当系统日志信息功能被启用后,默认状态下将存储在网络设备的缓存中。而网络设备一旦瘫痪,缓存中的日志文件将被全部丢失,除非事先将其保存至闪存中。因此,若欲借助日志文件分析故障和安全事件,必须将日志信息存储在其他目的设备。

设置日志信息存储设备配置过程如下。

(1) 进入全局配置模式。

```
Cisco# configure terminal
```

(2) 将日志信息记录到设备内置的缓存。默认缓存大小为 4096 字节,可取值范围为 4096～2147483647 字节。

提示:因为交换机其他任务也需要使用该缓存,建议不要将缓存设置得太大。使用 show memory 命令可以查看交换机中空闲的内存。size 的设置值一定要小于最大可用值。

```
Cisco(config)# logging buffered[size]
```

(3) 将日志记录到 UNIX 系统日志服务器。host 可以是系统日志服务器的计算机名称或 IP 地址。如果有多台 UNIX 系统日志服务器,应当重复执行该命令。

```
Switch(config)# logging host
```

（4）将系统日志保存在设备闪存中。max-file-size 用于指定日志文件的最大尺寸，取值范围为 4096～2147483647 字节，默认值为 4096 字节。min-file-size 用于指定日志文件的最小尺寸，取值范围为 1024～2147483647 字节，默认值为 2048 字节。severity-level-number | type，用于指定每个日志的严重级别或日志类型，取值范围为 0～7。

```
Cisco(config)# logging file flash:filename[max-file-size[min-file-size]] [severity-level-number|type]
```

提示：将日志保存在设备闪存中是个不错的选择。特别是当没有专门的 UNIX 系统日志服务器时。

（5）返回特权模式。

```
Cisco(config-line)# end
```

（6）校验配置。

```
Cisco# show running-config
```

（7）保存修改后的配置。

```
Cisco# copy running-config startup-config
```

3．配置日志消息的时间戳

当时间戳功能打开时，源设备发出的系统信息中有该信息产生时的日期和时间，该功能默认是打开本地时间，在没有系统时钟的设备上，默认是打开系统上的本地时间。在默认情况下，日志消息没有时间戳。

在特权 EXEC 模式下开始，启用 log 消息的时间标签。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）启用 log 时间标签。

```
Switch(config)# service timestamps log uptime
```

或

```
Switch (config)# service timestamps log datetime[msec][localtime][show-timezone]
```

（3）返回特权 EXEC 模式。

```
Switch(config-if)# end
```

（4）校验配置。

```
Switch# show running-config
```

（5）保存配置。

```
Switch# copy running-config startup-config
```

若要禁用调试和 log 消息的时间标签，可使用 no service timestamps 全局配置指令。

4．配置日志序列号

当序列号功能打开时，源设备发出的系统信息中有该信息产生的序列号值。默认情况

下，日志消息的序列号是不显示的。

在特权 EXEC 模式下开始，启用 log 消息的序列号。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）启用序列号。

```
Switch(config)# service sequence-numbers
```

（3）返回特权 EXEC 模式。

```
Switch(config-if)# end
```

（4）校验配置。

```
Switch# show running-config
```

（5）保存配置。

```
Switch# copy running-config startup-config
```

若欲禁用序列号，使用 no service sequence-numbers 全局配置命令即可。

5. 定义消息严重等级

可以限制将某种级别的消息发送至某种目的设备。在特权 EXEC 模式下开始，借助以下步骤可以定义消息的严重等级及目的设备。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）限制将消息发送到控制台。

```
Switch(config)# logging console level
```

（3）限制将消息发送到终端。

```
Switch(config)# logging monitor level
```

（4）限制将消息发送到日志服务器。

```
Switch(config)# logging trap level
```

（5）返回特权 EXEC 模式。

```
Switch(config-if)# end
```

（6）校验配置。

```
Switch# show running-config
```

或

```
Switch# show logging
```

（7）保存配置。

```
Switch# copy running-config startup-config
```

若欲禁用控制台上的日志，使用 no logging console 全局配置命令即可。若欲禁用到终端或其他控制台的日志，使用 no logging monitor 全局配置即可。若欲禁用系统日志陷阱，使用 no logging trap 全局配置命令即可。

6. 限制日志发送到历史表和 SNMP

将系统日志消息陷阱发送到 SNMP 网络管理站点后，使用 snmp-server enable trap 全局配置命令，可以改变发送消息的等级，并存储在交换机历史表中，也可以改变存储在历史表中消息的数量。消息被存储在历史表中，是因为 SNMP 陷阱不能保障每个消息都能到达目的地。默认情况下，一个警告等级的消息和低编号的等级被存储在历史表中，甚至系统日志陷阱也不被启用。

在特权 EXEC 模式下，按如下步骤可以改变等级和历史表默认大小。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 改变存储在历史文件中和发送到 SNMP 服务器的系统日志消息等级。

```
Switch(config)# logging history level
```

(3) 指定可以被存储在历史表中的系统日志消息的编号。

```
Switch(config)# logging history size number
```

(4) 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

(5) 校验配置。

```
Switch# show running-config
```

(6) 保存修改后的配置。

```
Switch# copy running-config startup-config
```

当历史表满时，最早的消息就会从表中删除，允许新消息被存储。

将系统 log 消息返回到默认等级，可以使用 no logging history 全局配置命令。返回在历史表中消息的编号到默认值，可以使用 no logging history size 全局配置命令。

7.2.7 IOS 系统版本升级

IOS 是 Cisco 拥有的核心软件数据包，主要在 Cisco 路由器和交换机上实现。IPS(入侵防御系统)则是包括 Cisco 路由器在内的许多网络产品具有的保护功能，能够实时阻止未经授权的网络访问和恶意代码。众所周知，Cisco IOS 难免会出现种种漏洞，某些情况下，恶意用户就可以利用 IOS 漏洞绕过 IPS 侵入系统，并影响 IPS 的正常运行，甚至使其瘫痪，从而导致“拒绝服务”攻击的发生。因此，路由器和交换机(尤其是路由器)必须及时为 IOS 安装升级补丁封堵漏洞。

1. 备份系统软件映像

为了保证网络设备系统映像在意外损坏(如误删除、闪存故障或被恶意攻击者破坏)和保障系统映像升级后,遇到问题时可以迅速恢复,应当及时备份系统软件映像,特别是在执行 IOS 系统升级前,必须要执行该操作。系统映像的备份需要借助 TFTP 服务器完成。下面以 Cisco 3640 系统映像的备份为例介绍。

(1) 运行 Cisco TFTP 服务器,通过 Console 端口、超级终端或 Telnet 登录至需要备份系统映像的网络设备。

提示: 充当 TFTP 服务器的计算机必须关闭网络防火墙,开启 TFTP 服务端口。并且交换机的 IP 访问列表中不能限制 TFTP 端口。

(2) 进入全局配置模式。

```
Cisco# configure terminal
```

(3) 查看当前闪存中的 IOS 系统版本,如图 7-1 所示。

```
Cisco# show version
```

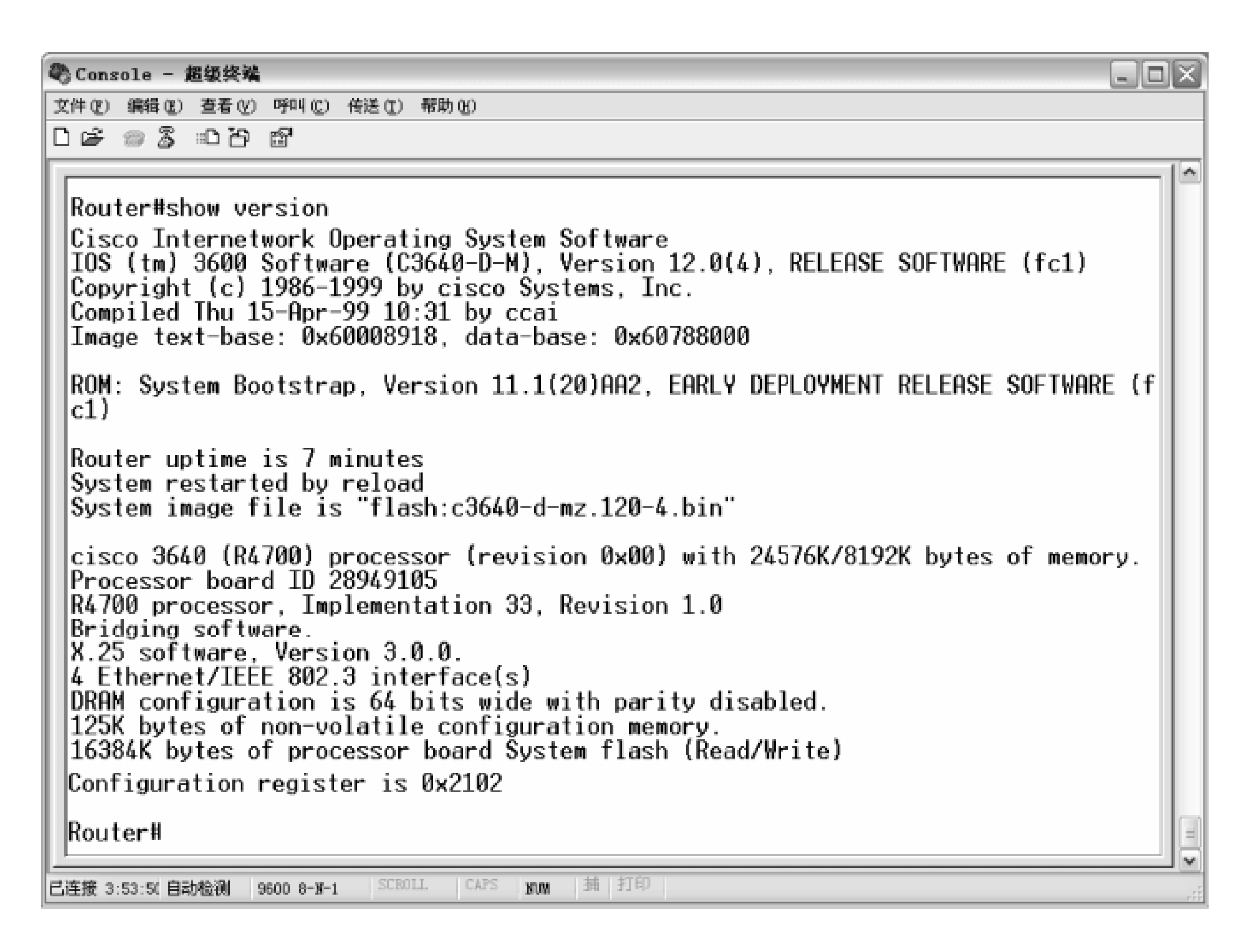


图 7-1 查看当前 IOS 系统版本

(4) 查看闪存中的文件夹和系统映像文件名称,如图 7-2 所示。确认系统文件名称为 c3640-d-mz.120-4.bin,IOS 映像文件的扩展名为.bin。

```
Cisco# dir flash:
```

提示: 如果系统文件位于子文件夹中,可以使用 cd sub_dir 命令进入该子文件夹,然后,再使用 dir 命令查看系统文件映像名称。

(5) 将软件映像上传至 TFTP 服务器,如图 7-3 所示。在提示符下,指定源 IOS 文件名、TFTP 服务器地址、目的 IOS 文件名和系统映像将被上传至 TFTP 服务器。

```
Cisco# copy flash tftp
```

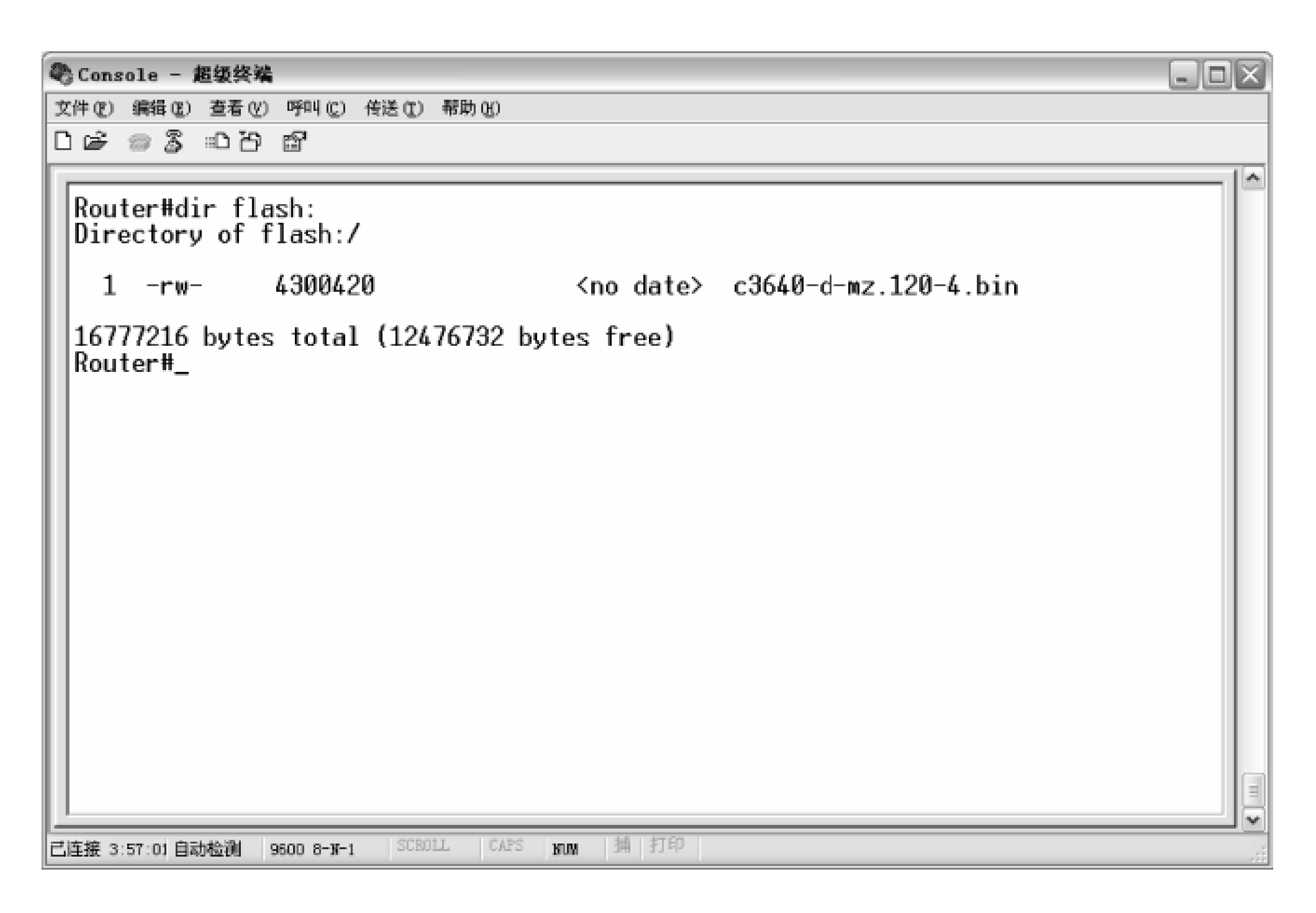


图 7-2　查看闪存文件系统

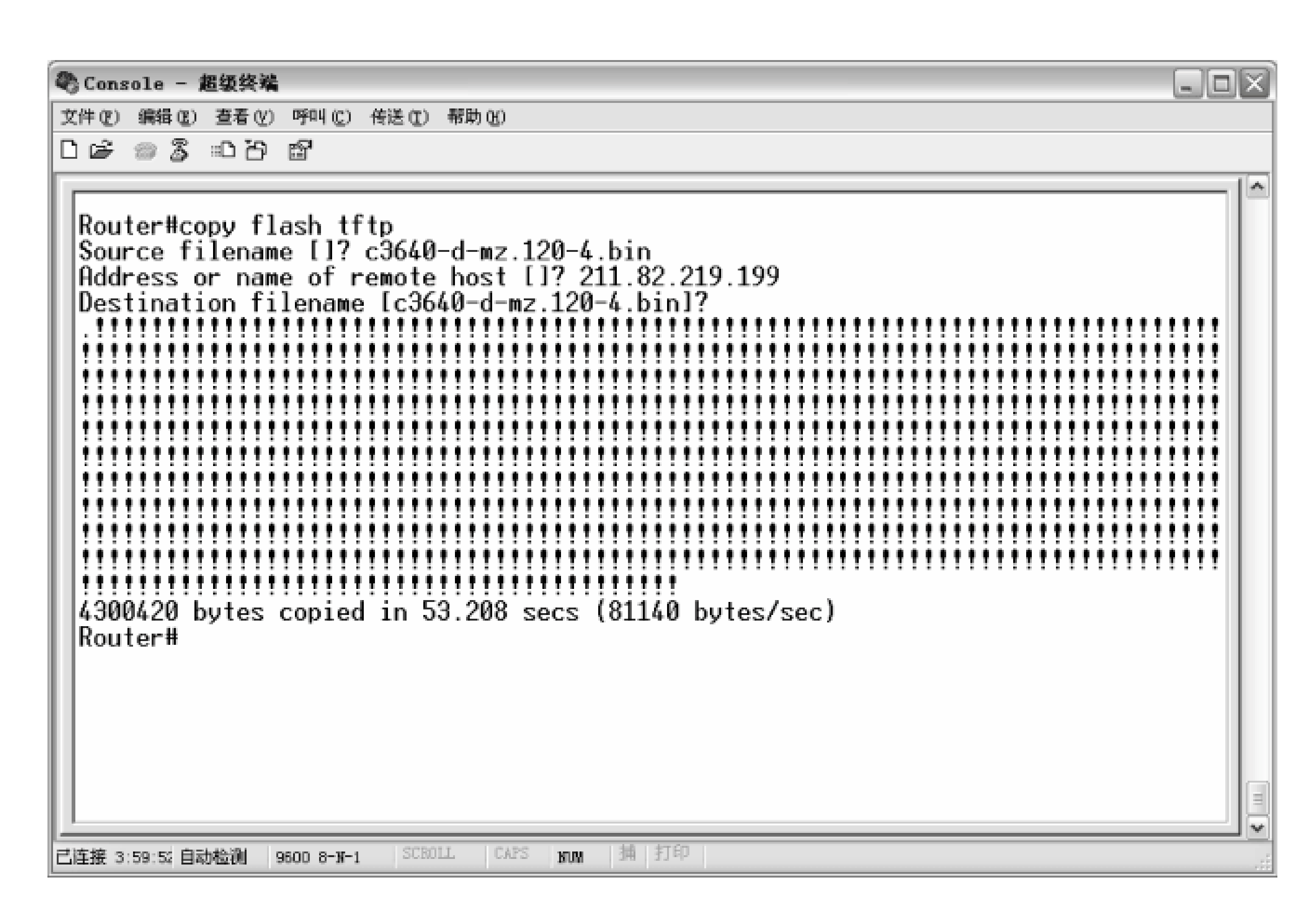


图 7-3　将 IOS 上传至 TFTP 服务器

2. 恢复或升级系统软件映像

使用 TFTP 服务器，可以通过网络将系统软件映像下载到网络设备。当软件映像下载时，该映像文件被下载至超级引擎闪存中。如果闪存的容量够大，可以在其中保存多个映像文件，并选择用于引导的映像文件。

(1) 将下载的软件映像复制至 Cisco TFTP 服务器默认目录(C:\program files\Cisco Systems\Cisco TFTP Server)。通过 Console 端口、超级终端或 Telnet 登录至交换机。如果使用 Telnet 登录交换机，那么，当交换机运行新软件而重新启动时，将断开连接。

提示：同时使用 Console 端口和以太网端口，连接管理计算机和要升级系统映像的网络设备，将大大提高系统映像的复制速度。

(2) 查看网络设备闪存容量，确认系统映像小于或等于该值。

```
Cisco# show flash:
```

（3）从 TFTP 服务器下载软件映像，如图 7-4 所示。在提示符下输入 TFTP 服务器的 IP 地址或主机名，以及要更新升级的 IOS 文件名，并确认删除原有的系统映像。网络设备将从 TFTP 服务器下载映像文件，并将映像复制到引导闪存。

Cisco＃ copy tftp flash

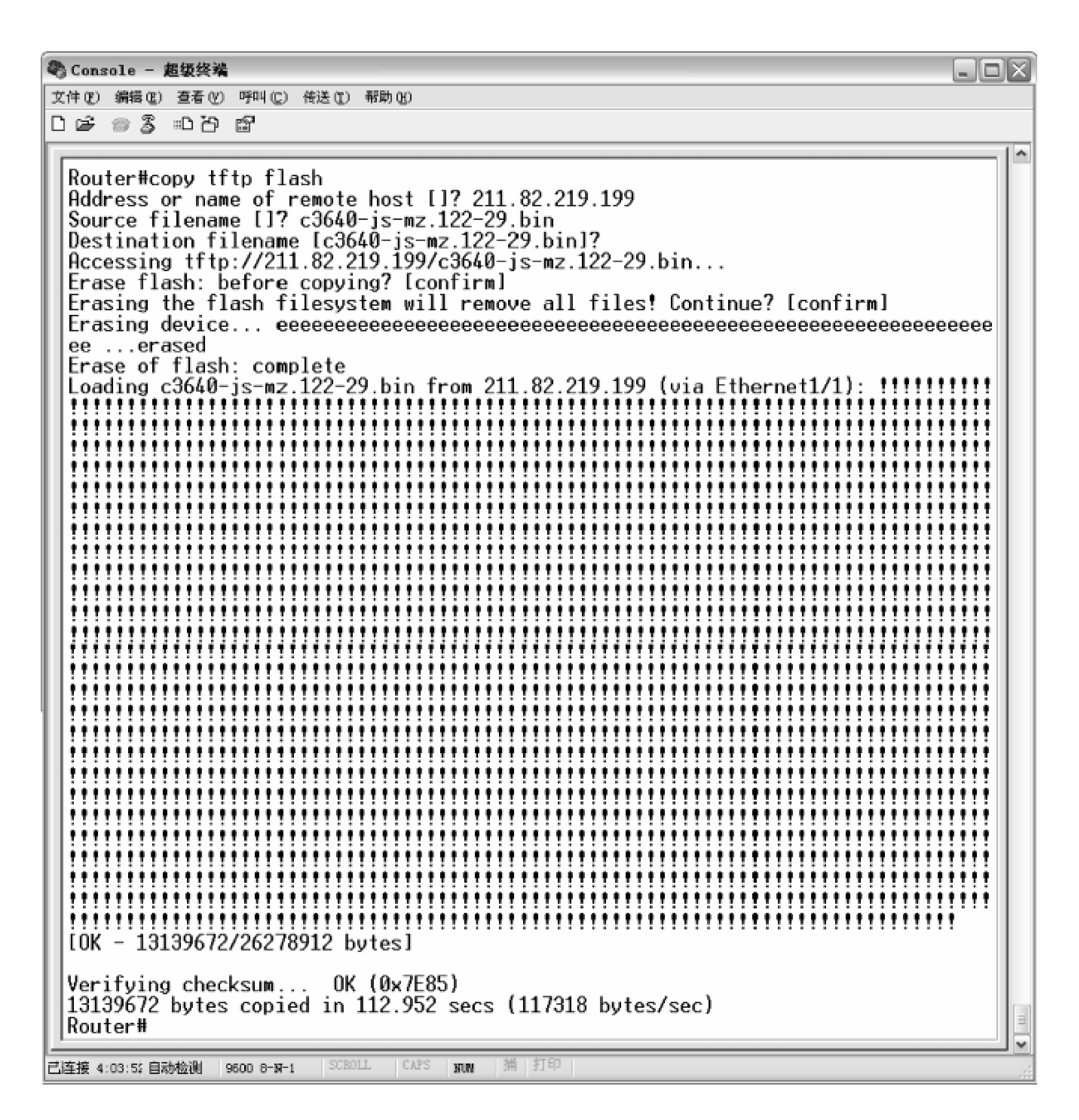


图 7-4 更新 IOS 系统映像

（4）重新引导 IOS 系统。

Cisco＃ reload

（5）按 Ctrl＋Break 键，中断网络设备的正常启动，进入 ROM 监视模式，如图 7-5 所示，指定用于引导的映像文件名称。

Cisco＃ boot flash:c3640-js-mz.122-29.bin

（6）再次重新引导 IOS 系统。

Cisco＃ reset

（7）查看更新的 IOS 版本，如图 7-6 所示。

7.2.8 知识链接：系统安全

1. IOS 登录密码

Cisco 的 Enable 密码有两种类型，即 secret password 和 password。其中，前者被加密存储，安全性较强，使用 show 命令不能查看到密码内容。而后者则未被加密，安全性较差，

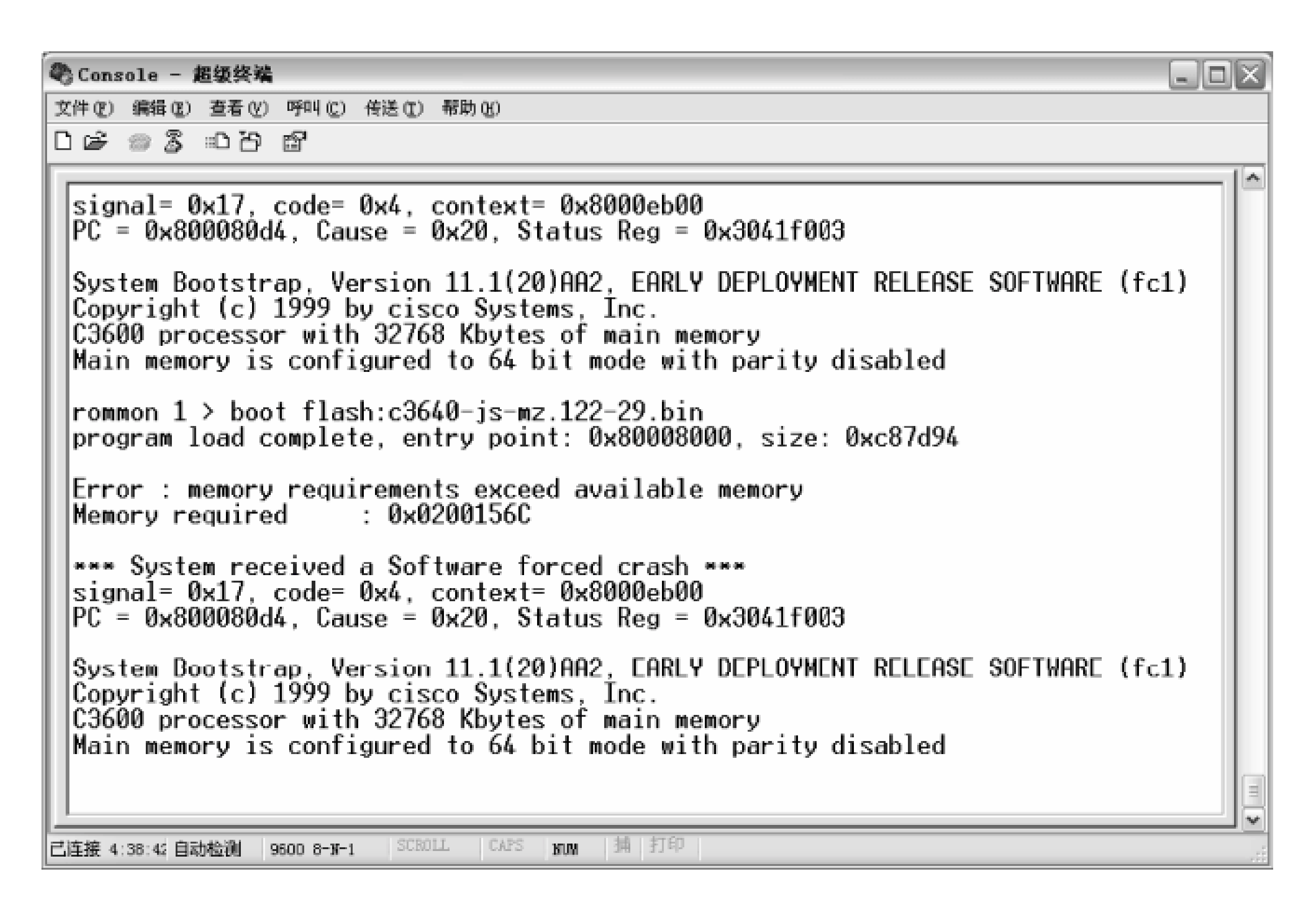


图 7-5 进入 ROM 监视模式

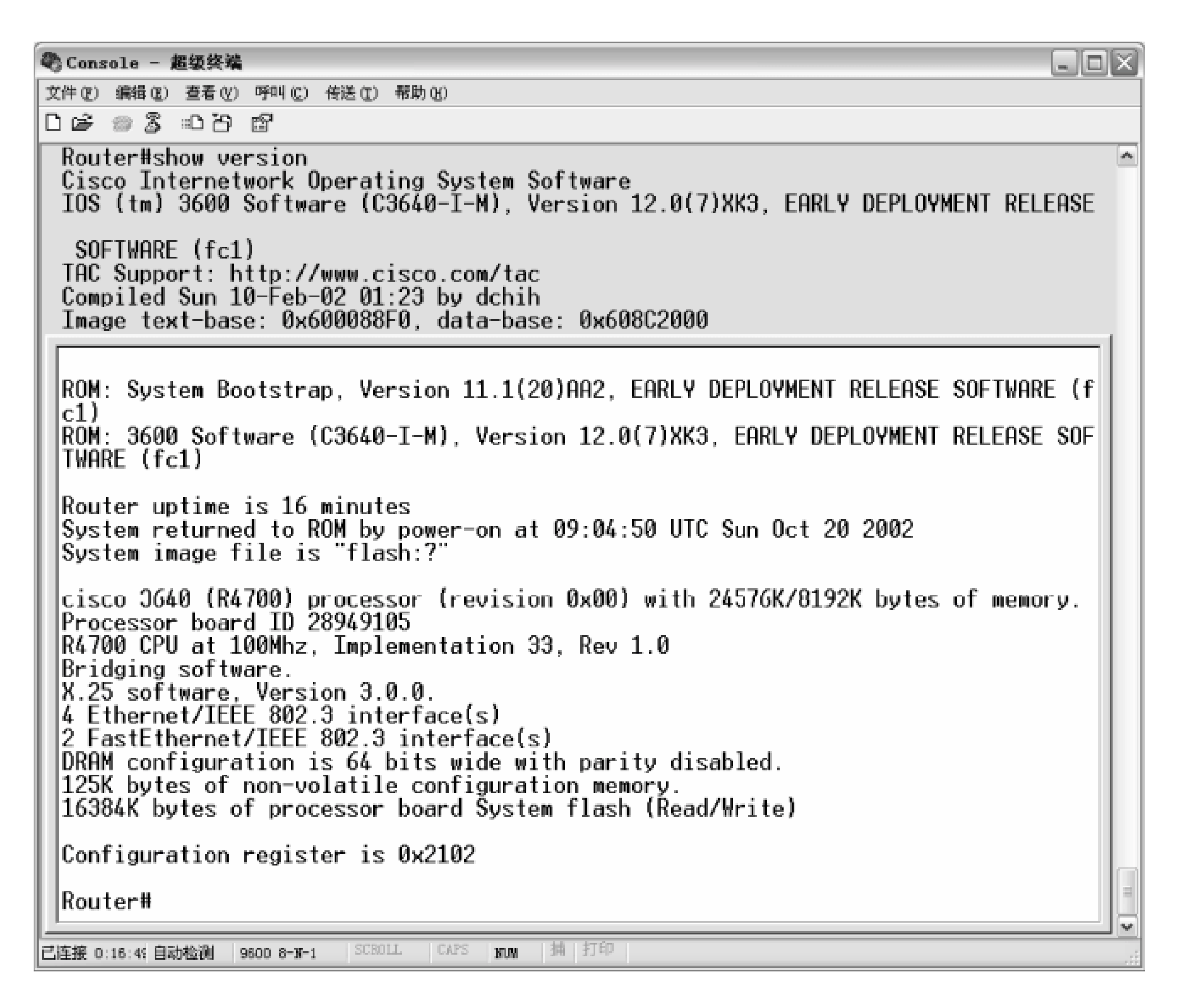


图 7-6 查看更新的 IOS 版本

可以使用 show 命令查看。因此，从安全的角度考虑，建议使用更加安全的 secret password。

secret password 较 password 的级别更高，当设置了 secret password 后，将不再能够使用 password。两种密码对大小写都敏感，即大写字母 A 与小写字母 a 是两种不同的符号，所以，必须牢记该密码。

2. 命令级别安全

在默认情况下，系统只有两个受口令保护的授权级别，即普通用户级别和特权用户级别。不过，可以为每个模式的命令划分 16 个授权级别。通过给不同的级别设置口令，就可以使不同的授权级别使用不同的命令集合。例如，想让更多的授权级别使用某一条命令，则可以将该命令的使用权授予较低的用户级别。而如果想让命令的使用范围小一些，则可以

将该命令的使用权授予较高的用户级别。

当在 Cisco IOS 中进入不同的权限等级时，权限等级越高，能进行的操作就越多。例如，用户在默认配置下登录到 Cisco 路由器或交换机的用户配置模式(最低权限级别)下时，只能查看某些信息(接口状态、路由信息等)，但不能进行任何修改或查看运行的配置文件。当需要修改 IOS 配置时，就必须凭借密码进入特权配置模式(最高权限级别)，此时用户即可对设备进行全面控制。

3. 终端访问限制

默认状态下，可以通过任何网络中的任意计算机登录到交换机或路由器。因此，必须将访问列表应用于虚拟终端线路上，使得拥有特定 IP 地址的用户才有权访问网络设备，建立 Telnet 会话。会话空闲超时限制主要用于确保建立会话后，管理员暂时离开控制台的连接空闲时间内的操作安全，严防恶意用户乘虚而入。

4. SNMP 协议安全

SNMP 是一种应用协议，为 SNMP 管理者和代理间的通信定义了协议消息格式。SNMP 管理者可以是网络管理系统的一部分，代理和管理信息库(MIB)包含在交换机上，通过配置交换机上的 SNMP，可以规定管理者同代理之间的联系。SNMP 代理包含 SNMP 管理者能够请求或更改的管理变量。管理者能够从代理那里获得管理变量值或者向代理设置管理变量值。代理从 MIB(包含设备的参数和网络数据信息)中收集管理信息。代理也能够响应管理者发出的设置或请求操作。代理能够向管理者主动发出 TRAP 信息。TRAP 信息是用来向管理者通告网络中的某种事件的发生。TRAP 信息能够通告认证失败、重启动、连接状态和拓扑改变等重要的事件的发生。

5. IOS 安全日志

日志是重要的系统资源，IOS 安全日志记录了网络设备运行的重要状态信息，是排除网络故障、检测安全漏洞的重要依据。根据时间、严重程度的不同，IOS 日志信息可以分为 0～7 级共 8 级，其中 0 级表示情况最严重。IOS 日志信息的现实格式如下：

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

7.3 交换机 IOS 安全配置

交换机是网络中最主要的集线设备，分布于整个网络的所有分支，因此通常也是网络管理员部署网络策略的最好选择。Cisco IOS 不仅适用于 Cisco 路由器，而且适用于 Cisco 三层和四层交换机，并且支持丰富的扩展功能，如远程监控、端口传输控制、VLAN 划分等。

7.3.1 基于端口的传输控制

借助对端口传输控制的配置，既可以有效杜绝广播风暴对整个网络的冲击，从而保证网络的正常通信。同时，又可以拒绝未被授权的计算机接入网络，或者限制某个端口接入计算机的数量，从而保证网络的接入安全，避免网络被个别用户滥用。

1. 风暴控制

当端口接收到大量的广播、单播或多播包时，就会发生广播风暴。转发这些包将导致网

络速度变慢或超时。同时,由于广播包被所有用户接收和处理,多播包也将被部分用户接收和处理,因此,也将大大降低服务器、客户计算机的处理能力。借助于对端口的广播风暴控制,可以有效地避免硬件损坏或链路故障导致的网络瘫痪。默认状态下,广播、多播和单播风暴控制被禁用,管理员可以按照如下操作启用端口的风暴控制。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

(3) 配置广播(broadcast)、多播(multicast)或单播(unicast)风暴控制。默认状态下,风暴控制被禁用。

① level:指定阻塞端口的带宽上限值。当广播、多播或单播传输占到宽带的多大比例(百分比)时,端口将阻塞传输。取值范围为0.00~100.00。如果将值设置为100%,将不限制任何传输;如果将值设置为0%,那么,该端口的所有广播、多播和单播都将被阻塞。

② level-low:指定启用端口的带宽下限值。该值应当小于或等于下限值,当广播、多播或单播传输占用带宽的比例低于该值时,端口恢复转发传输。取值范围为0.00~100.00。

③ bps:指定端口阻塞的传输速率上限值。当广播、多播或单播传输达到每秒若干比特(bps)时,端口将阻塞传输。取值范围为0.0~10000000000.0。

④ bps-low:指定端口启用的传输速率下限值。该值应当小于或等于下限值,当广播、多播或单播传输低于每秒若干比特(bps)时,端口将恢复传输。取值范围为0.0~10000000000.0。如果数值较大,也可以使用Kbps、Mbps或Gbps等单位表示。

⑤ pps:指定端口阻塞的转发速率上限值。当广播、多播或单播传输速率达到每秒若干包(pps)时,端口将阻塞传输。取值范围为0.0~10000000000.0。

⑥ pps-low:指定端口启用的传输速率下限值。该值应当小于或等于下限值,当广播、多播或单播转发速率低于每秒若干包(pps)时,端口将恢复传输。取值范围为0.0~10000000000.0。如果数值较大,也可以使用Kbps、Mbps或Gbps等单位表示。

```
Switch(config-if)# storm-control{broadcast|multicast|unicast}level{level[level-low]|bps bps[bps-low]|pps pps[pps-low]}
```

(4) 指定风暴发生时如何处理。默认状态下,将过滤外出的传输,并不发送SNMP陷阱。选择shutdown关键字,在风暴期间将禁用端口;选择trap关键字,当风暴发生时,产生一个SNMP陷阱,向网络管理软件发出警报。

```
Switch(config-if)# storm-control action{shutdown|trap}
```

(5) 返回特权配置模式。

```
Switch(config-if)# end
```

(6) 显示并校验该接口当前的配置。

```
Switch# show storm-control[interface][{broadcast|history|multicast|unicast}]
```

(7) 保存风暴控制配置。

```
Switch# copy running-config startup-config
```

提示:如果要禁用端口的风暴控制,则只需在端口配置模式下运行如下命令即可:

```
no storm-control{broadcast|multicast|unicast}
```

或者运行如下命令禁用指定的风暴控制动作:

```
no storm-control action{shutdown|trap}
```

2. 流量控制

当在交换机配置有 QoS(Quality of Service)时,不要再配置 IEEE 802.3x 流量控制。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 选择欲配置的端口,进入接口配置模式。

```
Switch(config)# interface interface-id
```

(3) 设置端口的流量控制模式。Receive on(或 desired)端口不能发送暂停帧,但是能够作为被请求设备工作,即该端口可以接收暂停帧。Receive off,流量控制在所有的方向均不工作。当拥塞发生时,不向链路伙伴发出指示,不发送和接收暂停帧。默认状态为 off。

```
Switch(config-if)# flowcontrol{receive}{on|off|desired}
```

(4) 返回特权配置模式。

```
Switch(config-if)# end
```

(5) 显示接口状态。

```
Switch# show interfaces interface-id
```

(6) 保存配置。

```
Switch# copy running-config startup-config
```

3. 传输速率限制

网络传输速率变低的主要原因,往往是某些用户对网络的滥用。当使用 MRTG 等流量监控软件检测到流量来源于某个端口时,可以在核心交换机、汇聚交换机,甚至接入交换机上,对相应的端口做必要的处理,限制其传输带宽,从而限制每个用户所允许的最大流量,以便使其他网络用户能够恢复正常的网络应用服务。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

(3) 配置端口带宽控制。其中,input/output 表明在输入和输出方向应用该带宽限制,

通常情况下，应当进行双向限制。access-group acl-index 用于定义使用该带宽限制的访问列表。bps 用于定义限制带宽，以 bps 为单位，并采用 8Kbps 的增量。burst-normal 用于定义所允许的普通突发速率，burst-max 用于定义所允许的最大突发速率。conform-action conform-action 用于指定在规定最大带宽时所执行的操作，通常为 transmit，即允许发送。exceed-action exceed-action 则用于指定在规定最大带宽时所执行的操作，通常为 drop，即丢弃。

```
Switch(config-if)# rate-limit{input|output}[access-group acl-index] bps burst-normal burst-max
conform-action conform-action exceed-action exceed-action
```

(4) 返回特权配置模式。

```
Switch(config-if)# end
```

(5) 显示并校验该接口当前的配置。

```
Switch# show interface interface-id
```

(6) 保存带宽限制配置。

```
Switch# copy running-config startup-config
```

例如，若欲限制 GigabitEthernet4/4 带宽为 128Kbps，当连接的普通突发速率、最大突发在 8K Bytes(即 64Kbps)至 9K Bytes(即 72Kbps)范围内时，所执行的操作是 transmit(传输即发送)；当超出该范围时，则相应的操作就是 drop。其中，128000 用于限制最大带宽，8000 和 9000 则用于限制突发连接，保证不因个别用户的大量传输而使整个链路性能大幅度下降。限制输入和输出速率后，该端口配置如下：

```
interface GigabitEthernet4/4
no switchport
description zhanshiting
ip address 172.16.100.3 255.255.255.0
ip access-group 120 in
ip access-group 120 out
rate-limit output access-group 102 128000 8000 9000 conform-action transmit exceed-action drop
rate-limit input access-group 102 128000 8000 9000 conform-action transmit exceed-action drop
```

IP 访问列表只需设置应用带宽限制的 IP 地址范围(192.168.0.0～192.168.255.255)即可，内容如下：

```
access-list 102 permit ip 192.168.0.0 0.0.255.255 any
```

注意：*在启用宽带限制之前，必须先在全局模式下执行 ip cef 命令，启用交换机的快速转发技术。*

4. 绑定 IP 和 MAC 地址

许多安全设置都是基于 IP 的，而用户的 IP 地址却可以随意设置。因此，还应当同时采取另外一种安全措施，即在交换机中将 IP 地址与 MAC 地址绑定在一起。这样，即使用户设置了 IP 地址，也由于 MAC 地址不同而不能获得相应的权限，从而保证网络的安全。

使用下述命令，可将 MAC 地址与 IP 地址绑定在一起。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）绑定 IP 地址与 MAC 地址。若欲绑定若干 IP 地址，需要重复该操作。

```
Switch(config-if)# arp ip-address mac-address arpa
```

（3）保存当前配置。

```
Switch# copy running-config startup-config
```

7.3.2 配置 VLAN 安全

VLAN 的主要作用有两点，一是提高网络安全性，阻止未经授权的 VLAN 访问；二是提高网络传输效率，将广播隔离在子网之内。因此，VLAN 在网络安全性和稳定性方面，都起着非常重要的作用。

1. 划分 VLAN

创建 VLAN 共需要两个步骤，先是创建 VLAN，然后，再将相关接口指定至该 VLAN。这个过程跟先划分若干部门，然后，再将人员一一分配至各部门非常相似。图 7-7 所示为在一台交换机上创建 4 个 VLAN，并将相应的端口指定至相应的 VLAN。

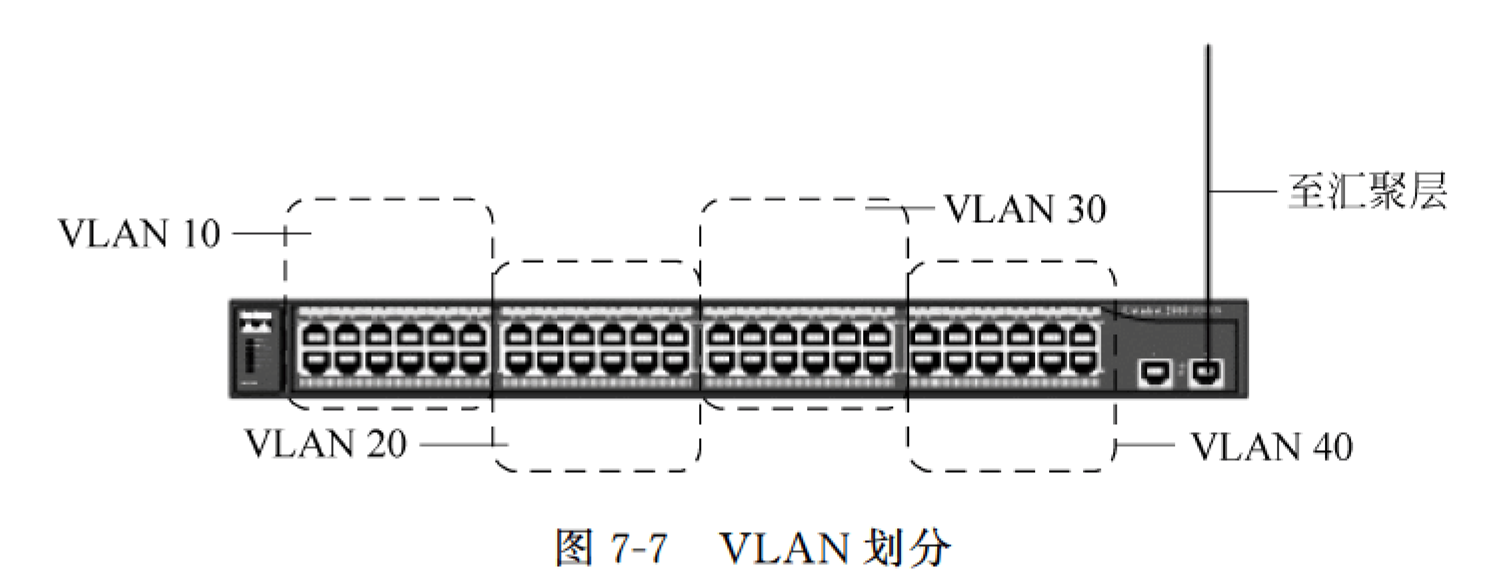


图 7-7 VLAN 划分

由于交换机默认只创建了一个管理 VLAN 1，因此，应当根据需要为每个部门都分别创建一个 VLAN。每个 VLAN 都需要创建。创建 VLAN 过程如下。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）输入 VLAN ID，进入 VLAN 配置模式。以太网 VLAN ID 的取值范围为 1～1001。其中，VLAN 1 为系统默认 VLAN，不能被创建，也不能被删除。

```
Switch(config)# vlan vlan-id
```

（3）（可选）为 VLAN 命名。如果不为 VLAN 命名，默认在 VLAN ID 前添加 0 作为 VLAN 名称。例如，VLAN 0080 是 VLAN 80 的默认命称。

```
Switch(config-vlan)# name vlan-name
```

（4）返回特权配置模式。

```
Switch(config-vlan)# end
```

（5）查看并检验 VLAN 配置。

```
Switch# show vlan[id|name]vlan-name
```

（6）保存 VLAN 配置。如果交换机处于 VTP 透明模式，VLAN 配置被保存在运行配置文件时，也被保存至 VLAN 数据库。这里只是将当前配置保存至启动配置。

```
Switch# copy running-config startup-config
```

2. 将端口指定至 VLAN

通常情况下，应当将同一部门的职员，或者拥有相同的访问权限，或者执行同一任务的用户，划分至同一 VLAN。当然，这里的用户直接表现为连接至某个端口的计算机。将端口指定至 VLAN 的过程如下。

（1）进入配置模式。

```
Switch# config terminal
```

（2）指定欲配置的接口。

```
Switch(config)# interface interface-id
```

（3）为端口（第二层访问端口）定义 VLAN 成员模式。

```
Switch(config-if)# switchport mode access
```

（4）将接口添加至指定的 VLAN。

```
Switch(config-if)# switchport access vlan vlan-id
```

（5）退出接口配置模式。

```
Switch(config-if)# end
```

（6）显示并校验该接口当前的配置。

```
Switch# show interface interface-id
```

（7）保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

提示：若欲将多个端口指定至某个 VLAN，必须一一重复执行上述命令。或者采用指定端口组的方式，一次将多个端口指定至同一 VLAN。

3. 清除接口配置

当用户所在的部门发生变化，或者端口所连接的计算机发生变化时，可以直接使用 switchport access vlan vlan-id 命令，将端口指定至新的 VLAN。不过，如果需要将接口配置为 Trunk，或者三层接口时，则需要先清除接口配置。事实上，只需将指定接口恢复为默认值，即可清除该接口的所有配置。

（1）进入 VLAN 配置模式。

```
Switch# config terminal
```

（2）清除某接口的所有配置。

```
Switch(config)# default interface interface-id
```

（3）返回特权配置模式。

```
Switch(config)# end
```

（4）保存对配置的修改。

```
Switch# copy running-config startup-config
```

4. 删除 VLAN

当某个部门被撤销，或者不再需要某个 VLAN 时，可以将该 VLAN 删除。使用 no vlan vlan-id 命令，可删除指定的 VLAN。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）选择欲删除的 VLAN。

```
Switch(config)# vlan vlan-id
```

（3）删除指定的 VLAN。

```
Switch(config-vlan)# no vlan vlan-id
```

（4）更新 VLAN 数据库，并返回特权配置模式。

```
Switch(config-vlan)# end
```

（5）校验 VLAN 的改变。

```
Switch(config-vlan)# show vlan brief
```

（6）保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

注意：删除 VLAN 后，所有指定至 VLAN 的端口将不再可用，直到将其指定至新 VLAN 时止。

5. 设置 VLAN Trunk 过滤

当在交换机上划分有多个 VLAN 时，若欲借助一条链路实现与其他交换机的通信，就必须要创建 Trunk（如图 7-8 所示）。默认状态下，第二层接口自动处于动态的 Switchport 模式，当相邻接口（即借助于双绞线或光纤连接在一起的两个端口）支持 Trunk，并且配置为 Trunk 或动态匹配模式，该链接即可作为 Trunk 链接。默认状态下，Trunk 端口允许所有 VLAN 的发送和接口传输。当然，根据需要，也可以拒绝某些 VLAN 通过 Trunk 传输，从而将限制该 VLAN 与其他交换机的通信，或者拒绝某些 VLAN 对敏感数据的访问。

VLAN Trunk 配置过程如下。

（1）进入全局配置模式。

```
Switch# configure terminal
```

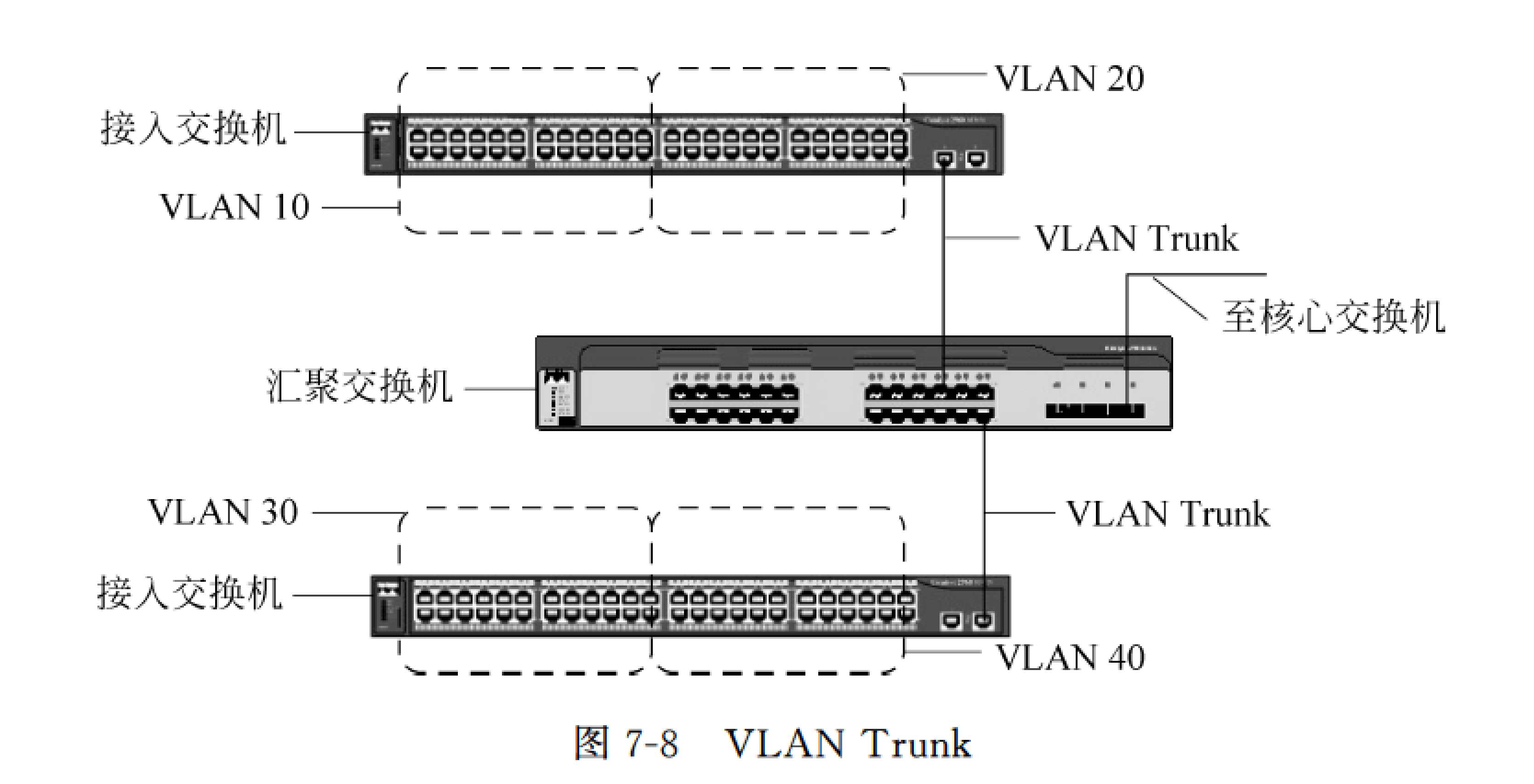


图 7-8 VLAN Trunk

(2) 指定欲配置的接口。

```
Switch(config)# interface interface-id
```

(3) 将接口配置为第二层 Trunk。只有接口是第二层访问接口,或者指定 Trunk 模式时,才需要使用该命令。dynamic auto,如果相邻接口被设置为 trunk 或 desirable 模式,将该接口置为 Trunk 连接。dynamic desirable,如果相邻接口设置为 trunk、desirable 或 auto 模式,将该接口置为 Trunk 连接。trunk,将接口设置为永久 Trunk 模式,协商将连接转换为 Trunk 连接,即使相邻接口不是 Trunk 接口。

```
Switch(config-if)# switchport mode{dynamic{auto|desirable} |trunk}
```

(4) (可选)指定默认 VLAN,即当 Trunk 停止后,将使用哪一个 VLAN。既可指定某一个 VALN,也可以指定一个 VLAN 范围。访问 VLAN 不能作为本地 VLAN 使用。

```
Switch(config-if)# switchport access vlan vlan-id
```

(5) 为 802.1Q Trunk 指定本地 VLAN。不指定本地 VLAN,默认将使用VLAN 1。

```
Switch(config-if)# switchport trunk native vlan vlan-id
```

(6) 配置 Trunk 上允许的 VLAN 列表。需要注意的是,不能从 Trunk 中移除默认的 VLAN 1。使用 add(添加)、all(所有)、except(除外)和 remove(移除)关键字,可以定义允许在 Trunk 上传输的 VLAN。VLAN 列表既可以是一个 VLAN,也可以是一个 VLAN 组。当同时指定若干 VLAN 时,不要在“,”或“-”间使用空格。

```
Switch(config-if)# switchport trunk allowed vlan{add|all|except|remove}vlan-list
```

若欲允许所有 VLAN 都通过该 Trunk,可以使用 no switchport trunk allowed vlan 接口配置命令。

(7) 返回至特权配置模式。

```
Switch(config-if)# end
```

(8) 查看并校验配置。

```
Switch# show interface interface-id switchport
```

```
Switch# show interfaces interface-id trunk
```

（9）保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

若欲将接口恢复至默认值，可以使用 default interface interface-id 接口配置命令。若欲将 Trunk 接口中的所有特征恢复为默认值，可以使用 no switchport trunk 接口配置命令。若欲禁用 Trunk，可以使用 switchport mode access 接口配置命令，端口将作为一个静态访问端口。

7.3.3 配置 PVLAN 安全

配置 PVLAN 安全的主要操作步骤如下。

（1）将 VTP 模式设置为透明模式，即禁用 VTP。

（2）创建辅 VLAN。

（3）创建主 VLAN。

（4）为主 VLAN 与辅 VLAN 建立关联。一个独立 VLAN 可以与一个主 VLAN 关联，多个团体 VLAN 可以与主 VLAN 关联。

（5）将接口配置为独立或团体端口。

（6）将独立端口或团体端口关联为主-辅 VLAN 对。

（7）将接口配置为混杂端口。

（8）将混杂端口映射为主-辅 VLAN 对。

1. 将 VLAN 配置为 PVLAN

使用以下操作步骤，将 VLAN 配置为 PVLAN。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）指定欲设置为 PVLAN 的 VLAN。

```
Switch(config)# vlan vlan-ID
```

（3）将指定 VLAN 设置为 PVLAN，并指定 PVLAN 类型。在退出 VLAN 配置模式时，该配置命令不会生效。

```
Switch(config-vlan)# private-vlan{isolated|primary}
```

（4）返回特权配置模式。

```
Switch(config)# end
```

（5）校验当前设置。

```
Switch# show vlan private-vlan[type]
```

（6）保存当前配置。

```
Switch# copy running-config startup-config
```

2. 关联主 VLAN 与辅 VLAN

使用以下操作步骤，关联主 VLAN 与辅 VLAN。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定主 VLAN，进入 VLAN 配置模式。

```
Switch(config)# vlan primary-vlan-ID
```

(3) 建立辅 VLAN 与主 VLAN 的关联。该列表只能包括一个 VLAN。

```
Switch(config-vlan)# private-vlan association{secondary-vlan-list|add secondary-vlan-list|remove secondary-vlan-list}
```

(4) 返回特权配置模式。

```
Switch(config)# end
```

(5) 校验当前设置。

```
Switch# show vlan private-vlan[type]
```

(6) 保存当前配置。

```
Switch# copy running-config startup-config
```

当关联辅 VLAN 和主 VLAN 时，需要注意以下几点。

① secondary-vlan-list 参数只能包含一个 Isolated VLAN ID。

② 使用 remove 关键字可以清除辅 VLAN 与主 VLAN 的关联。该列表包括一个 VLAN。

③ 只有退出 VLAN 配置模式时，输入的命令才会生效。

3. 配置 PVLAN 混杂端口

使用以下操作步骤，配置 PVLAN 混杂端口。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定欲配置的二层端口。

```
Switch(config)# interface interface-id
```

(3) 将二层接口配置为 PVLAN 混杂端口。

```
Switch(config-if)# switchport mode private-vlan{host|promiscuous|trunk}
```

(4) 将 PVLAN 混杂端口映射为主 VLAN，并选择辅 VLAN。

```
Switch(config-if)# switchport private-vlan mapping primary-vlan-id {secondary-vlan-list | add secondary-vlan-list|remove secondary-vlan-list}
```

(5) 返回特权配置模式。

```
Switch(config)# end
```

(6) 校验当前设置。

```
Switch# show interfaces interface-id switchport
```

(7) 保存当前配置。

```
Switch# copy running-config startup-config
```

在将二层接口配置为 PVLAN 混杂端口时,需要注意以下几点。

① secondary-vlan-list 参数不能有空格,也不能包括由多个“,”分隔开的条目。每个条目只能包括一个 PVLAN ID 或一个带有“-”的 PVLAN ID 范围。

② 输入 secondary-vlan-list 或使用 add 关键字,将辅 VLAN 映射到 PVLAN 混杂端口。

③ 使用 remove 关键字可以清除辅 VLAN 和 PVLAN 混杂端口的关联。

4. 配置 PVLAN Host 端口

使用以下操作步骤,配置 PVLAN 主机端口。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定欲配置的二层端口。

```
Switch(config)# interface interface-id
```

(3) 将二层接口配置为 PVLAN 主机端口。

```
Switch(config-if)# switchport mode private-vlan{host|promiscuous}|trunk
```

(4) 将二层接口关联至 PVLAN。

```
Switch(config-if)# switchport private-vlan host-association primary-vlan-id secondary-vlan-id
```

(5) 返回特权配置模式。

```
Switch(config)# end
```

(6) 校验当前设置。

```
Switch# show interfaces interface-id switchport
```

(7) 保存当前配置。

```
Switch# copy running-config startup-config
```

5. 配置 PVLAN Trunk 端口

使用以下操作步骤,配置 PVLAN Trunk 端口。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定欲配置的二层端口。

```
Switch(config)# interface interface-id
```

(3) 将二层接口配置为 PVLAN Trunk 端口，实现多个辅 PVLAN 在一条链路上的传输。

```
Switch(config-if)# switchport mode private-vlan{host|promiscuous|trunk}
```

(4) 建立主 VLAN 与辅 VLAN 的关联，将 PVLAN 端口作为一个 PVLAN。使用该命令，可以指定多个 PVLAN 对，从而使 PVLAN Trunk 端口实现多个辅 VLAN 的传输。如果关联被指定至一个已有的 VLAN，现有关联将被替换。如果没有创建 Trunk 关联，辅 VLAN 上接收的任何包都将被丢弃。

```
Switch(config-if)# switchport private-vlan association trunk primary-vlan-id secondary-vlan-id
```

(5) 在 PVLAN Trunk 端口配置普通 VLAN 的允许列表。

```
Switch(config-if)# switchport private-vlan trunk allowed vlan vlan-list all|none|[add|remove|
except]vlan-atom[,vlan-atom...]
```

(6) 将 VLAN 配置为非标签包。如果没有本地 VLAN，所有非标签包将被丢弃。如果本地 VLAN 是辅 VLAN，并且端口没有与辅 VLAN 关联，非标签包也将被丢弃。

```
Switch(config-if)# switchport private-vlan trunk native vlan vlan-id
```

(7) 返回特权配置模式。

```
Switch(config)# end
```

(8) 校验当前设置。

```
Switch# show interfaces interface-id
```

(9) 保存当前配置。

```
Switch# copy running-config startup-config
```

6. 将辅 VLAN 映射为主 VLAN 三层 VLAN 接口

若欲借助三层交换机实现 PVLAN 间的路由，必须为主 VLAN 配置 SVI(Switch Virtual Interface，交换机虚拟接口)，并且将辅 VLAN 映射至 SVI。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定欲配置的 Primary VLAN，进入接口配置模式。

```
Switch(config)# interface vlan primary-vlan-id
```

(3) 将 Secondary VLAN 映射至三层 VLAN 接口，从而允许 PVLAN 在三层交换机上实现数据传输。

```
Switch(config-if)# private-vlan mapping primary-vlan-id{secondary-vlan-list|add secondary-vlan-list
| remove secondary-vlan-list}
```

(4) 返回特权配置模式。

```
Switch(config)# end
```

(5) 校验当前设置。

```
Switch# show interface private-vlan mapping
```

(6) 保存当前配置。

```
Switch# copy running-config startup-config
```

7.3.4 配置 RMON

1. 默认的 RMON 配置

交换机 RMON 支持 SNMP 的 1、2、3、9 组内容。

(1) 统计组。统计组(statistics)是 RMON 中的第 1 组,统计组统计被监控的每个子网的基本统计信息。目前只能对网络设备的以太网接口进行监控和统计。

(2) 历史组。历史组(history)是 RMON 中的第 2 组,历史组定期地收集统计网络值的记录并为日后的处理把统计存储起来。它包含两个小组。其中,HistoryControl 组用来设置采样间隔时间等控制信息;EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。

(3) 警报组。警报组(alarm)是 RMON 中的第 3 组,以指定的时间间隔监控一个特定的 MIB(Management Information Base)对象,当这个 MIB 对象的值超过一个设定的上限值或低于一个设定的下限值时,会触发一个警报。警报被当作事件来处理,处理事件的方式可以是记录日志或发送 SNMP Trap(陷阱)的方式。

(4) 事件组。事件组(event)是 RMON 中的第 9 组,决定当由于警报而产生事件时,处理行为是产生一个日志记录表项或者一个 SNMP Trap。

RMON 在默认情况下是禁用的,警告和过滤都没有被配置。在交换机上只有 RMON 1 被支持。

2. 配置 RMON 警报和事件

可以使用 CLI 或 SNMP 网络管理工作站配置交换机 RMON。建议使用 NMS(网络管理工作站)上的一般的 RMON 管理工具来实现 RMON 的管理,以便充分利用 RMON 的网络管理功能。当然,也必须在交换机上配置 SNMP 以访问 RMON MIB 对象。

在特权 EXEC 模式下开始,启用 RMON 警告和过滤。

(1) 进入全局配置模式。

```
Switch # configure terminal
```

(2) 设置针对一个 MIB 对象的报警功能。number 用于指定这个 alarm 表项的索引,取值范围是 1~65535。variable 表示要监控的 MIB 的变量标识符,该变量必须是整型类数据类型。interval 用于指定采样的时间间隔,单位为秒,取值范围为 1~2147483647s。关键字 delta 表示取样的值,指 MIB 变量在两次取样间值的变化;关键字 absolute 表示直接使用 MIB 变量的值作为取样值。value 用于指定警报触发的条件,即当 MIB 变量的值变化成大

于关键字 rising-threshold 后面指定的 value 值(从小于这个值变成大于这个值),或者变成小于关键字 falling-threshold 后面指定的 value 值时即触发警报。value 后所跟的值取值范围是-2147483648～2147483647。event-number(可选)表示报警引发的事件产生时,指定事件组产生事件表项的索引,若不指定则不会产生相应的事件。这个值的取值范围为1～65535。string(可选)用于标识这个报警表项的拥有者。

```
Switch(config)# rmon alarm number variable interval{absolute|delta} rising-threshold value[event-number]falling-threshold value[event-number][owner string]
```

(3) 当警报产生时,增加相应的事件表项并做相应的处理。number 表示事件表项的索引,和上面设置的 event-number 对应。一个警报产生时,若警报指定的 event-number 对应的事件表项(number 等于 event-number)不存在,则不会产生对应的事件。该值的取值范围为1～65535。log(可选)输入这个关键值,则警报产生时,会将这个事件记录到日志中。trap(可选)输入这个关键值,则警报产生时,会产生一个 SNMP Trap。community(可选)发送 trap 时使用的认证名。description string(可选)对这个事件的描述。owner string(可选)标志这个事件的拥有者。

```
Switch(config)# rmon event number[description string][log][owner string][trap community]
```

(4) 返回特权 EXEC 模式。

```
Switch(config)# end
```

(5) 校验配置。

```
Switch# show running-config
```

(6) 保存配置。

```
Switch# copy running-config startup-config
```

禁用警告,使用 no rmon alarm number 全局配置命令,不能立即禁用所有已配置的警告。禁用事件,使用 no rmon event number 全局配置命令。

3. 创建历史表组项

必须首先配置 RMON 警告和事件来显示收集的信息。

在特权 EXEC 模式下开始,下面的步骤是在接口上创建历史表组项。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定要收集历史表的接口,并进入接口配置模式。

```
Switch(config)# interface interface-id
```

(3) 创建历史表组项。index 用于指定这个历史记录配置表项的索引,值的范围是1～65535。owner ownername(可选)标志这个表项的拥有者。buckets 表示每次采样的数据将被保存下来,bucket-number 的值指定了保存每次采样数据的历史记录的最大表项个数。如果历史记录已满,则新的采样数据将覆盖最老的一次采样数据记录。取值范围是

1～65535，默认值为 10。interval 指定采样的时间间隔，单位为秒，范围为 1～3600s，默认为 1800s。

```
Switch(config-if)# rmon collection history index[buckets bucket-number][interval seconds][owner ownername]
```

(4) 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

(5) 校验配置。

```
Switch# show running-config
```

(6) 显示交换机历史中表的内容。

```
Switch(config)# show rmon history
```

(7) 保存配置。

```
Switch# copy running-config startup-config
```

禁用历史收集，使用 no rmon collection history index 接口配置命令。

4. 创建 RMON 统计组表项

可以针对物理端口设置统计表项。当设置了一个端口的统计表项后，交换机将从这时开始各种数据的统计。

在特权 EXEC 模式下，可以通过以下步骤来创建一个 RMON 统计组表项。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定创建统计组表项的接口，并进入接口配置模式。

```
Switch(config)# interface interface-id
```

(3) 创建 RMON 统计组表项。index 指定这个统计表项的索引，值的范围是 1～65535。owner ownername(可选)标志这个表项的拥有者。

```
Switch(config-if)# rmon collection stats index[owner ownername]
```

(4) 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

(5) 校验配置。

```
Switch# show running-config
```

(6) 显示交换机统计表的收集量。

```
Switch# show rmon statistics
```

(7) 保存配置。

```
Switch# copy running-config startup-config
```

禁用以太网组统计量的收集，使用 no rmon collection stats index 接口配置命令。

5. 显示 RMON 的状态

使用下述命令，可以显示 RMON 的状态。

(1) show rmon：显示全部的 RMON 统计。

(2) show rmon alarms：显示 RMON 警告表。

(3) show rmon events：显示 RMON 事件表。

(4) show rmon history：显示 RMON 历史表。

(5) show rmon statistics：显示 RMON 统计表。

7.3.5 知识链接：交换机 IOS 安全配置

1. VLAN

VLAN(Virtual Local Area Network，虚拟局域网)用于将端口指定至不同的子网，从而隔离彼此之间的广播和直接通信，提高网络传输效率和安全性。Trunk 则用于借助一个接口实现不同交换机之间多 VLAN 的传输。在局域网络中使用 VLAN 技术，具有以下重要意义和作用。

(1) 降低移动和变更的管理成本。VLAN 中的成员与其物理位置无关，既可连接至同一台交换机，也可连接至不同交换机。当需要把一台计算机从一个子网转移到另一个子网，迁移工作将只是由网络管理员在用作网络管理的计算机上重新定义 VLAN 成员。

(2) 控制广播。由于所有的广播都只在本 VLAN 内进行，而不再扩散到其他 VLAN 上，所以将大大减少广播对网络带宽的占用，提高带宽传输效率，并可有效地避免广播风暴的产生。

(3) 增强安全性。VLAN 的一个重要好处就是提高了网络安全性。由于交换机只能在同一 VLAN 内的端口之间交换数据，不同 VLAN 的端口不能直接相互访问。因此，通过划分 VLAN，就可以在物理上防止某些非授权用户访问敏感数据。

(4) 网络监督和管理的自动化。由于网络管理员可以通过网管软件，查到 VLAN 间和 VLAN 内通信的数据报的细目分类信息，以及应用数据报的细目分类信息，而这些信息对于确定路由系统，和经常遭到访问的服务器的最佳配置十分有用。通过划分 VLAN，可以使网络管理变得更简单、更轻松、更有效。

2. PVLAN

与 VLAN 不同，PVLAN 不仅与 VLAN 之间隔离，而且 PVLAN 内的端口之间也相互隔离，仅可通过上联端口访问网络。若用户希望端口之间通信，必须借助三层交换机或路由器进行路由转发。PVLAN 技术在解决通信安全、防止广播风暴和浪费 IP 地址方面的优势是显而易见的，而且采用 PVLAN 技术有助于网络的优化。另外，PVLAN 的配置也相对简单，不必占用 VLAN 资源。

3. RMON

RMON(Remote Monitor)远程监控是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。它为网络管理员选择符合指定网络需求的控制台和网络监控探测器提供了更多的自由。

7.4 路由器 IOS 安全配置

路由器主要用于处理局域网与 Internet，内部不同网络之间的信息传输，主要用于提供路径选择。由于路由器的硬件配置比较低，通常只配置必要的路由信息和基本的安全配置，如访问控制列表、NAT、NetFlow 等。Cisco 路由器使用与 Cisco 交换机相同的 Cisco IOS，因此，应用于交换机的许多功能和配置命令（如访问列表等），也同样适用于路由器。

7.4.1 配置访问列表

通常情况下，管理员可以按照如下步骤配置访问列表。

① 分析需求，搞清楚需要保护什么或控制什么；为方便配置，推荐以表格形式列出。

② 分析符合条件的数据流的路径，寻找一个最适合进行控制的位置。

③ 编写 ACL，并将 ACL 应用到接口上。

④ 测试并修改 ACL。

1. IP 访问列表

（1）创建标准访问列表

① 进入全局配置模。

```
Router# configure terminal
```

② 使用源地址或通配符定义标准 IP 访问列表。

```
Router(config)# access-list access-list-number{deny|permit}source[source-wildcard]
```

- access-list-number：ACL 号。ACL 号相同的所有 ACL 形成一个组。在判断一个包时，使用同一组中的条目从上到下逐一进行判断，一旦遇到满足条件的条目就终止对该包的判断。1～99 或 1300～1999 为标准的 IP ACL 号。
- deny|permit：当条件匹配时，是允许包通过，还是将包丢弃。
- source：源地址。发送包的网络或主机地址，使用点分十进制表示。当表示一组主机时，使用通配符屏蔽码。
- source-wildcard：通配符屏蔽码。Cisco 访问列表所支持的通配符屏蔽码与子网掩码的方式是相反的。也就是说，二进制“0”表示一个匹配条件，“1”表示一个不关心条件。

any 表示任何主机，即源地址和源通配符屏蔽码 0.0.0.0 255.255.255.255 的缩写。例如，若要拒绝从源地址 192.168.1.100 发出的报文，但允许发自其他源地址的报文，应当使用下述语句：

```
Access-list 1 deny host 192.168.1.100
Access-list 1 permit any
```

需要注意这两条语句的顺序。访问列表语句的处理是由上至下的。如果将两个语句顺序颠倒，将 permit 语句放在 deny 语句前面，则不能过滤来自主机的报文，因为 permit 语句将允许所有报文通过。访问列表中的语句顺序非常重要，不合理的语句顺序将会在网络中

产生安全漏洞，或者使得用户不能很好地利用公司的网络策略。

host 表示一台主机，是源和源通配符 0.0.0.0 的缩写。例如，若要允许从 192.168.1.200 发出的报文，则应当使用下述语句：

```
Access-list 1 permit 192.168.1.200 0.0.0.0
```

上述语句也可以使用下面的语句代替：

```
Access-list 1 permit host 192.168.1.200
```

③ 返回特权配置模式。

```
Router(config)# end
```

④ 校验当前设置。

```
Router# show access-lists number
```

⑤ 保存当前配置。

```
Router# copy running-config startup-config
```

使用 no access-list access-list-number 全局配置命令，可以删除全部访问列表。需要注意的是，不能从指定的访问列表中删除某个 ACE。

（2）创建扩展访问控制列表

标准 IP 访问控制列表只能控制源 IP 地址，不能控制到端口。若要控制企业用户的网络应用，就需要使用扩展 IP 访问控制列表。

① 进入全局配置模式。

```
Router# configure terminal
```

② 定义扩展 IP 访问控制列表，取值范围为 100～199 或 2000～2699。

```
Router(config)# access-list access-list-number {deny | permit} protocol source source-wildcard [operator port] destination destination-wildcard [operator port]
```

或

```
access-list access-list-number {deny | permit} protocol any [operator port] any [operator port]
```

或

```
access-list access-list-number {deny | permit} protocol host source [operator port] host destination [operator port]
```

protocol 要过滤的协议，例如 IP、TCP、UDP 和 ICMP 等。默认过滤所有协议，若要根据特殊协议进行报文过滤，需指定协议。

destination destination-wildcard 为目的地址和通配符屏蔽码。

operator 端口操作符，在协议类型为 TCP 或 UDP 时支持端口比较，支持的比较操作有：等于(eq)、大于(gt)、小于(lt)、不等于(neq)或介于(range)。如果操作符为 range，则后面需要跟两个端口。

port 端口号,可以用几种不同方法指定。可以显式地指定数字或使用一个可识别的助记符。例如,可以使用 80 或 HTTP 指定超文本传输协议,使用 21 或 FTP 指定文件传输协议。例如,若要允许来自任何地址的包含有 SMTP 数据的报文到达 192.168.10.10 主机,可以在访问列表中添加下述语句:

```
Access-list 101 permit tcp any host 192.168.10.10 eq smtp
```

③ 返回特权配置模式。

```
Router(config)# end
```

④ 校验当前设置。

```
Router# show access-lists number
```

⑤ 保存当前配置。

```
Router# copy running-config startup-config
```

(3) 将 IP 访问列表应用到接口

如果不将 IP 访问列表应用到接口,那么,该访问列表将不会发生作用。

① 进入全局配置模式。

```
Router# configure terminal
```

② 指定要应用该 IP 访问列表的接口。该接口既可以是二层接口(端口访问列表),也可以是三层接口(路由访问列表)。

```
Router(config)# interface interface-id
```

③ 将访问控制应用到指定的接口。二层接口(端口访问列表)不支持 out 关键字。

```
Router(config-if)# ip access-group{access-list-number|name}{in|out}
```

④ 返回特权配置模式。

```
Router(config-if)# end
```

⑤ 校验当前设置。

```
Router# show running-config
```

⑥ 保存当前配置。

```
Router# copy running-config startup-config
```

2. VLAN 访问列表

VLAN 映射是控制过滤 VLAN 内流量的唯一手段。VLAN 映射没有方向。若欲利用 VLAN 映射过滤特定方向上的流量,必须在 ACL 中配置指定的源或目的地址。与路由器 ACL 不同,VLAN 映射的默认操作是允许转发。如果包在映射中没有找到与之相匹配的条目,则将其转发出去。

创建一个 VLAN 映射,并将其配置至一个或多个 VLAN 的步骤如下。

① 创建将要应用到 VLAN 的标准 IP 访问控制列表或扩展 IP 访问控制列表，或命令 MAC 扩展访问控制列表。

② 输入全局配置命令 vlan access-map，创建 VLAN ACL 映射条目。

③ 在访问映射配置模式下，选择输入一种操作方式，可以是丢弃或转发，并输入 match 命令在一个或多个列表中匹配。

④ 使用全局配置命令 vlan filter，将 VLAN 映射配置到一个或多个 VLAN 上。

注意：VLAN 映射列表最后默认的操作是允许转发。也就是说，如果包在映射中没有找到与之相匹配的任何条目，则将其转发。

(1) 创建 VLAN 访问列表

借助以下操作，可以创建 VLAN 访问列表。

① 进入全局配置模式。

```
Router # configure terminal
```

② 创建 VLAN 映射，并给该 VLAN 访问列表定义一个名称和序号（可选），进入 VLAN 访问列表配置模式。当创建相同名称的 VLAN 映射时，会随之创建相应的序号，号码以 10 为级差递增。若欲修改或删除映射，直接输入映射条目的序号即可。

```
Router(config)# vlan access-map name[number]
```

③ 为 VLAN 映射设置动作，默认为转发（forward）。

```
Router(config-access-map)# action{drop|forward}
```

④ 借助一个或多个标准 IP 访问控制列表或扩展 IP 访问控制列表匹配包（使用 IP 或 MAC 地址）。IP 包只能被标准 IP 访问控制列表或扩展 IP 访问控制列表匹配；非 IP 包只能被 MAC 扩展 IP 访问控制列表匹配。

```
Router(config-access-map)# match{ip|mac}address{name|number}[name|number]
```

⑤ 返回特权配置模式。

```
Router(config-if)# end
```

⑥ 校验当前设置。

```
Router# show running-config
```

⑦ 保存当前配置。

```
Router# copy running-config startup-config
```

如下所示为创建 ACL 及 VLAN 映射以拒绝转发 TCP 流量。先创建 IP ACL 以允许所有的 TCP 包，然后，设置匹配该表项的包操作为丢弃。

```
Router(config)# ip access-list extended ip1
Router(config-ext-nacl)# permit tcp any any
Router(config-ext-nacl)# exit
Router(config)# vlan access-map map_1 10
Router(config-access-map)# match ip address udp
```

```
Router(config-access-map)# action drop
```

如下所示为创建允许 UDP 包通过的 VLAN 映射。

```
Router(config)# ip access-list extended ip2
Router(config-ext-nacl)# permit udp any any
Router(config-ext-nacl)# exit
Router(config)# vlan access-map map_1 20
Router(config-access-map)# match ip address udp2
Router(config-access-map)# action forward
```

如下所示为非 UDP 包全部被丢弃的 VLAN 映射。

```
Router(config)# vlan access-map map_1 30
Router(config-access-map)# action drop
```

(2) 将 VLAN 访问列表应用到 VLAN

借助以下操作,可以将 VLAN 访问列表应用到 VLAN。

① 进入全局配置模式。

```
Router# configure terminal
```

② 将 VLAN 映射应用至一个或多个 VLAN。可以使用"-"或","指定若干 VLAN。需要注意的是,"-"或","前后必须输入空格。

```
Router(config)# vlan filter mapname vlan-list list
```

③ 校验当前设置。

```
Router# show running-config
```

④ 保存当前配置。

```
Router# copy running-config startup-config
```

7.4.2 配置 NAT

NAT 被广泛应用于各种类型的 Internet 接入方式和各种类型的网络。原因是 NAT 不仅完美地解决 IP 地址不足的问题,而且还能有效地避免来自网络外部的攻击,隐藏并保护网络内部的计算机。配置 NAT 时应注意区分内部接口和外部接口,通常情况下,连接到企业网络的接口是 NAT 内部接口,而连接到外部网络(如 Internet)的接口是 NAT 外部接口。

1. 静态地址转换

所谓静态地址转换,是指将合法 IP 地址一一对应地转换为内部私有 IP 地址。如果企业网络获得多个合法 IP 地址,可以借助静态地址转换方式,将合法 IP 地址转换为内部服务器的 IP 地址,从而实现对企业网络和 Internet 对服务器的访问。

内部网络使用的 IP 地址段为 192.168.100.1~192.168.100.254,路由器局域网端口(即默认网关)的 IP 地址为 192.168.100.1,子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 121.17.46.128~121.17.46.135,路由器广域网中的 IP 地址为 121.17.46.129,子网掩码为 255.255.255.248,可用于转换的 IP 地址为 121.17.46.133。要求将内部网址

192.168.100.2～192.168.100.6 分别转换为合法 IP 地址 121.17.46.130～121.17.46.134。

(1) 设置外部端口。

```
interface serial 0/0
ip address 121.17.46.133 255.255.255.248
ip nat outside
```

(2) 设置内部端口。

```
interface fastethernet 0/0
ip address 192.168.100.1 255.255.255.0
ip nat inside
```

(3) 在内部本地地址与内部合法地址之间建立静态地址转换。

```
ip nat inside source static 内部本地地址,即内部合法地址
```

示例:

```
ip nat inside source static 192.168.100.2 121.17.46.130
!--将内部网络地址 192.168.100.2 转换为合法 IP 地址 121.17.46.130
ip nat inside source static 192.168.100.3 121.17.46.131
!--将内部网络地址 192.168.100.3 转换为合法 IP 地址 121.17.46.131
ip nat inside source static 192.168.100.4 121.17.46.132
!--将内部网络地址 192.168.100.4 转换为合法 IP 地址 121.17.46.132
ip nat inside source static 192.168.100.5 121.17.46.133
!--将内部网络地址 192.168.100.5 转换为合法 IP 地址 121.17.46.133
ip nat inside source static 192.168.100.6 121.17.46.134
!--将内部网络地址 192.168.100.6 转换为合法 IP 地址 121.17.46.134
```

至此,静态地址转换配置完毕。

2. 动态地址转换

所谓动态地址转换,是指将内部私有 IP 地址动态地转换为合法 IP 地址池内的 IP 地址,对应关系是不固定的。如果企业网络获得多个合法 IP 地址,可以借助动态地址转换方式,实现 Internet 连接共享。

内部网络使用的 IP 地址段为 172.16.100.1～172.16.100. 254,路由器局域网端口(即默认网关)的 IP 地址为 172.16.100.1,子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 121.17.46.128～121.17.46.191,路由器广域网中的 IP 地址为 121.17.46.129,子网掩码为 255.255.255.192,可用于转换的 IP 地址范围为 121.17.46.130～121.17.46.190。要求将内部网址 172.16.100.1～172.16.100. 254 动态转换为合法 IP 地址 121.17.46.130～121.17.46.190。

(1) 设置外部端口。

设置外部端口命令的语法如下:

```
ip nat outside
```

示例:

```
interface serial 0/0
```

```
!--进入串行端口 serial 0/0
ip address 121.17.46.129 255.255.255.248
!--将其 IP 地址指定为 121.17.46.129,子网掩码为 255.255.255.248
ip nat outside
!--将串行口 serial 0/0 设置为外网端口
```

需要注意的是,可以定义多个外部端口。

(2) 设置内部端口。

设置内部接口命令的语法如下:

```
ip nat inside
```

示例:

```
interface fastethernet 0/0
!--进入快速以太网端口 FastEthernet 0/0
ip address 172.16.100.1 255.255.255.0
!--将其 IP 地址指定为 172.16.100.1,子网掩码为 255.255.255.0
ip nat inside
!--将 FastEthernet 0/0 设置为内网端口
```

需要注意的是,可以定义多个内部端口。

(3) 定义合法 IP 地址池。

定义合法 IP 地址池命令的语法如下:

```
ip nat pool 地址池名称 起始 IP 地址 终止 IP 地址 子网掩码
```

其中,地址池名字可以任意设定。

示例:

```
ip nat pool chinanet 121.17.46.130 121.17.46.190 netmask 255.255.255.192
!--指定地址缓冲池的名称为 chinanet,IP 地址范围为 121.17.46.130～121.17.46.190
!--子网掩码为 255.255.255.192.需要注意的是,即使掩码为 255.255.255.0
!--也会由起始 IP 地址和终止 IP 地址对 IP 地址池进行限制。
!--或 ip nat pool test 121.17.46.130 121.17.46.190 prefix-length 26
```

(4) 定义内部网络中允许访问 Internet 的访问列表。

定义内部访问列表命令的语法如下:

```
access-list 标号 permit 源地址 通配符
```

其中,标号为 1～99 之间的整数。

```
access-list 1 permit 172.16.100.0 0.0.0.255
!--允许访问 Internet 的网段为 172.16.100.0～172.16.100.255,主机掩码为 0.0.0.255。
```

需要注意的是,在这里采用的是主机掩码,而非子网掩码。子网掩码与主机掩码的关系为:主机掩码+子网掩码=255.255.255.255。例如,子网掩码为 255.255.0.0,则主机掩码为 0.0.255.255;子网掩码为 255.0.0.0,则主机掩码为 0.255.255.255;子网掩码为 255.252.0.0,则主机掩码为 0.3.255.255;子网掩码为 255.255.255.192,则主机掩码为 0.0.0.63。

另外，如果想将多个 IP 地址段转换为合法 IP 地址，可以添加多个访问列表。例如，当欲将 172.16.98.0～172.16.98.255 和 172.16.99.0～172.16.99.255 转换为合法 IP 地址时，应当添加下述命令：

```
access-list 2 permit 172.16.98.0 0.0.0.255
access-list 2 permit 172.16.99.0 0.0.0.255
```

(5) 实现网络地址转换。

在全局设置模式下，将由 access-list 指定的内部本地地址与指定的内部合法地址池进行地址转换。命令语法如下：

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字
```

示例：

```
ip nat inside source list 1 pool chinanet
```

如果有多个内部访问列表，可以一一添加，以实现网络地址转换，如：

```
ip nat inside source list 2 pool chinanet
ip nat inside source list 2 pool chinanet
```

至此，动态地址转换设置完毕。

3. 端口复用地址转换

所谓端口复用地址转换，是指将通过复用 TCP 端口的方式，使用一个合法 IP 地址实现 Internet 连接共享。如果企业网络只获得一个合法的 IP 地址，则应当采用端口复用地址转换方式。

内部网络使用的 IP 地址段为 10.100.100.1～10.100.100.254，路由器局域网端口(即默认网关)的 IP 地址为 10.100.100.1，子网掩码为 255.255.255.0。路由器广域网中的 IP 地址为 202.99.160.1，子网掩码为 255.255.255.248。要求将内部网址 10.100.100.1～10.100.100.254 转换为合法 IP 地址。

(1) 进入全局配置模式。

```
Router# configure terminal
```

(2) 设置外部端口。

```
Router(config)# interface serial 0/0
Router(config-if)# ip address 202.99.160.1 255.255.255.252
Router(config-if)# ip nat outside
```

(3) 返回全局配置模式。

```
Router(config-if)# exit
```

(4) 设置内部快速以太网端口。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 1.100.100.1 255.255.255.0
Router(config-if)# ip nat inside
```

（5）返回全局配置模式。

```
Router(config-if)# exit
```

（6）设置复用动态地址转换，复用广域口合法 IP 地址。

```
Router(config)# ip nat inside source list 120 interface Serial0/0 overload
!--指明复用串行口的合法 IP 地址，访问列表为 120
```

（7）定义内部访问列表。

```
Router(config)# access-list 120 permit ip 10.100.100.1.0 0.0.0.255 any
!--定义 120 访问列表，允许访问 Internet 的网段为 10.100.100.0～10.100.100.255
!--子网掩码为 255.255.255.0，主机掩码为 0.0.0.255
```

在全局设置模式下，设置在内部的本地地址与内部合法 IP 地址间建立复用动态地址转换。命令语法如下：

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字 overload
```

示例：

```
ip nat inside source list 1 pool public overload
!--以端口复用方式，将访问列表 1 中的私有 IP 地址转换为 public IP 地址池中定义的合法 IP 地址。
```

（8）返回 Enable 模式。

```
Router(config)# end
```

（9）保存配置。

```
Router# running-config startup-config
```

至此，端口复用动态地址转换完成。

7.4.3 配置 NetFlow

NetFlow 工作过程中使用路由器的时间来标记流数据，所以路由器上的时间准确与否非常重要。NetFlow 可以自动处理不同时区的路由器。当 NetFlow 服务器的时间和路由器的时间存在 10min 以上的误差时，将在主页上显示警告图标。此时 NetFlow 分析仪将使用 NetFlow 分析仪服务器本身的时间来标记流。在路由器上输出 NetFlow 数据前，首先需要启用 NetFlow 输出，然后设置 NetFlow 数据目的输出地址。

启用 NetFlow 输出的配置如下。

（1）进入接口配置模式。

```
Router(config)# interface{interface}{interface_number}
```

（2）启用 NetFlow 输出。

```
Router(config-if)# ip route-cache flow
```

（3）设置带宽信息参数（可选）。

```
Router(config-if)# bandwidth <Kbps>
```

(4) 退出接口配置模式。

```
Router(config-if)# exit
```

设置输出 NetFlow 数据到 NetFlow 分析仪所运行的服务器上的操作如下。

(1) 输出 NetFlow 缓存条目到指定的 IP 地址,使用 NetFlow 分析仪服务器的 IP 地址以及在配置 NetFlow 监听端口中所配置的端口,NetFlow Analyzer 默认使用端口为 9996。

```
Router(config)# ip flow-export destination{hostname|ip_address}9996
```

(2) 设置输出到指定 IP 地址的 NetFlow 输出中的源 IP 地址。NetFlow 分析仪将在此设备上执行 SNMP 请求。

```
Router(config)# ip flow-export source{interface}{interface_number}
```

(3) 设置 NetFlow 输出的版本为版本 5。NetFlow 分析仪只支持版本 5 和 7。如果路由器使用 BGP,则可以指定是否在输出包含源或者对方不可能包含两者。

```
Router(config)# ip flow-export version 5[peer-as|origin-as]
```

(4) 分割活动期长的流为 1min 的片段。可以选择 1～60min。如果使用默认的 30min,则流量报告可能会产生许多尖峰。这里为了生成警告和显示故障排除数据设定该值为 1min。

```
Router(config)# ip flow-cache timeout active 1
```

(5) 保证定期输出完成的流。默认值为 15s,可以选择 10～600s。如果选择的值大于 250s,NetFlow 分析仪将报告流量值太低的错误信息。

```
Router(config)# ip flow-cache timeout inactive 15
```

(6) 全局启用 ifIndex 持续化。这将保证 ifIndex 值在设备重启后也有效。

```
Router(config)# snmp-server ifindex persist
```

(7) 返回配置模式。

```
Router(config)# end
```

(8) 查看 NetFlow 的配置。

```
Router# show ip flow export
```

这里以在路由器上执行的命令集为例进行介绍,设置接口 GigabitEthernet 0/1 输出 NetFlow 版本 5 到 211.82.218.243 的 9996 端口。

```
2821ccme# enable
Password:
2821ccme# configure terminal
2821ccme(config)# interface GigabitEthernet 0/1
2821ccme(config-if)# ip route-cache flow
```

```
2821ccme(config-if)# exit
2821ccme(config)# ip flow-export destination 211.82.218.243 9996
2821ccme(config)# ip flow-export source GigabitEthernet 0/1
2821ccme(config)# ip flow-export version 5
2821ccme(config)# ip flow-cache timeout active 1
2821ccme(config)# ip flow-cache timeout inactive 15
2821ccme(config)# snmp-server ifindex persist
2821ccme(config)# end
2821ccme# copy running-config startup-config
2821ccme# show ip flow export
```

7.4.4 知识链接：路由器 IOS 安全配置

1. ACL

ACL(Access Control List,访问控制列表)是 Cisco IOS 提供的一种访问控制技术,被广泛应用于路由器和三层交换机。借助 ACL,可以有效地控制用户对网络和 Internet 的访问,从而最大限度地保障网络安全。Cisco 支持如下 3 种类型的访问列表。

(1) 标准 IP 访问控制列表。此类访问列表只允许过滤源地址,且功能十分有限。可以用于阻止来自某一网络的所有通信流量,或者允许来自某一特定网络的所有通信流量。

(2) 扩展 IP 访问控制列表。此类访问列表允许过滤源地址、目的地址和上层应用数据,因此可以适应各种复杂的网络应用。扩展 IP 访问控制列表既检查数据包的源地址,也检查数据包的目的地址,还检查数据包的特定协议类型、端口号等。

(3) 命名访问控制列表。在标准 IP 访问控制列表与扩展 IP 访问控制列表中均要使用表号,而在命名访问控制列表中使用一个字母或数字组合的字符串来代替前面所使用的数字。

在设置访问列表时,应当遵循最小特权原则,即只给受控对象完成任务所必需的最小权限,从而最大限度地保障网络传输安全。每个 ACL 中都包含一个 ACE(Access Control Entry,访问控制条目)规则列表,每个 ACE 都指定 permit(允许)或 deny(拒绝),以及应用条件,报文会逐个条目顺序匹配 ACE。访问列表表项的检测是按照自上而下的顺序进行的,因此,应用时应注意 ACL 中 ACE 的先后顺序。

2. NAT

NAT(Network Address Translation,网络地址转换)是常用的 Internet 接入方式之一,其实现方式有如下 3 种。

(1) 静态转换,是指将内部网络的私有 IP 地址转换为公用 IP 地址时,IP 地址对是一对一的,是一成不变的,某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换,可实现外部网络对内部网络中某些特定设备(如服务器)的访问。

(2) 动态转换,是指将内部网络的私有 IP 地址转换为公用 IP 地址时,IP 地址对是不确定的,是随机的,所有被授权访问 Internet 的私有 IP 地址,可随机转换为任何指定的合法 IP 地址。也就是说,只要指定哪些内部地址可以进行转换,以及用哪些合法地址作为外部地址时,就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时,可以采用动态转换的方式。

(3) 端口多路复用,是指改变外出数据包的源端口并且进行端口转换完成,即端口地址转换(Port Address Translation,PAT)。采用端口多路复用方式,内部网络的所有主机均可

共享一个合法外部 IP 地址，实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式了。

3. NetFlow

NetFlow 是 Cisco 公司开发的网络流量分析工具，一个 NetFlow 系统包括 3 个主要部分：探测器、采集器、报告系统。探测器是用来监听网络数据的。采集器是用来收集探测器传来的数据的。报告系统是用来从采集器收集到的数据产生易读的报告的。

并不是所有的 Cisco 设备均支持 NetFlow，并且支持 NetFlow 的设备所支持的版本也有所不同。具体支持 NetFlow 的 Cisco 设备类型如表 7-1 所示。

表 7-1 支持 NetFlow 的 Cisco 设备类型和 IOS 版本

Cisco IOS 软件发布版本	支持的 Cisco 硬件平台
11.1CA，11.1CC	Cisco 7200 及 7500 系列，RSP 7200 系列
12.0	Cisco 1720，2600，3600，4500，4700，AS5800 RSP 7000 及 7200 系列 uBR 7200 及 7500 系列 RSM 系列
12.0T，12.0S	Cisco 1720，2600，3600，4500，4700，AS5800 RSP 7000 及 7200 系列 uBR 7200 及 7500 系列 RSM 系列，MGX8800RPM 系列，及 BPx8600 系列
12.0(3)T，12.0(3)S	Cisco 1720，2600，3600，4500，4700，AS5300，AS5800 RSP 7000 及 7200 系列 uBR 7200 及 7500 系列 RSM 系列，MGX8800RPM 系列，BPx8650 系列
12.0(4)T	Cisco 1400，1600，1720，2500，2600，3600，4500，4700，AS5300，AS5800 RSP 7000 及 7200 系列 uBR 7200 及 7500 系列 RSM 系列，MGX8800RPM 系列，BPx8650 系列
12.0(4)XE	Cisco 7100 系列
12.0(6)S	Cisco 12000 系列

另外，Cisco 800、1700、1800、2800、3800、6500、7300、7600、10000、CRS-1，以及 Catalyst 系列的 4500 系列、5500 系列、6000 系列交换机也支持 NetFlow。而对于使用 NetFlow 功能卡（NFFC）或 NFFC Ⅱ 及路由交换模块（RSM），或路由交换功能卡（RSFC）的交换机，也可支持 NetFlow，但需要检查是否支持版本 5，因为多数交换机默认输出版本 7。

7.5 无线接入点安全配置

无线 AP（Access Point，接入点）的作用类似于以太网络中的交换机，用于实现无线客户端之间的信号中继和互联。几乎所有的无线 AP 都支持 Web、Telnet 以及图形窗口管理方式，从而简化了网络设备的管理难度。本案例中，无线 AP 主要部署在展示厅中，设备型

号为 Cisco Aironet 1300。下面,以 Cisco Aironet 1300 无线网桥(无线网桥也是无线 AP 的一种)为例介绍一下无线 AP 的常规安全设置。

7.5.1 配置 SSID

默认状态下,无线 AP 生产商会利用 SSID(初始化字符串),来检验企图登录无线网络节点的连接请求,一旦检验通过,即可顺利连接到无线网络。由于同一厂商的产品都使用相同的 SSID 名称,从而给恶意攻击者提供了入侵的条件。一旦他们使用通用的初始化字符串来连接无线网络时,就很容易建成一条非授权链接,从而给无线网络的安全带来威胁。因此,必须修改默认的 SSID 初始化字符串,提高设备安全性。以 Cisco Aironet 1300 无线网桥为例,配置 SSID 的主要操作如下。

(1) 以管理员账户登录到 Cisco Aironet 1300 无线网桥 Web 管理窗口后,单击左侧导航栏中的 SECURITY,即可查看当前的各项安全设置,如图 7-9 所示,继续进入下面的相关配置页面即可修改安全设置。

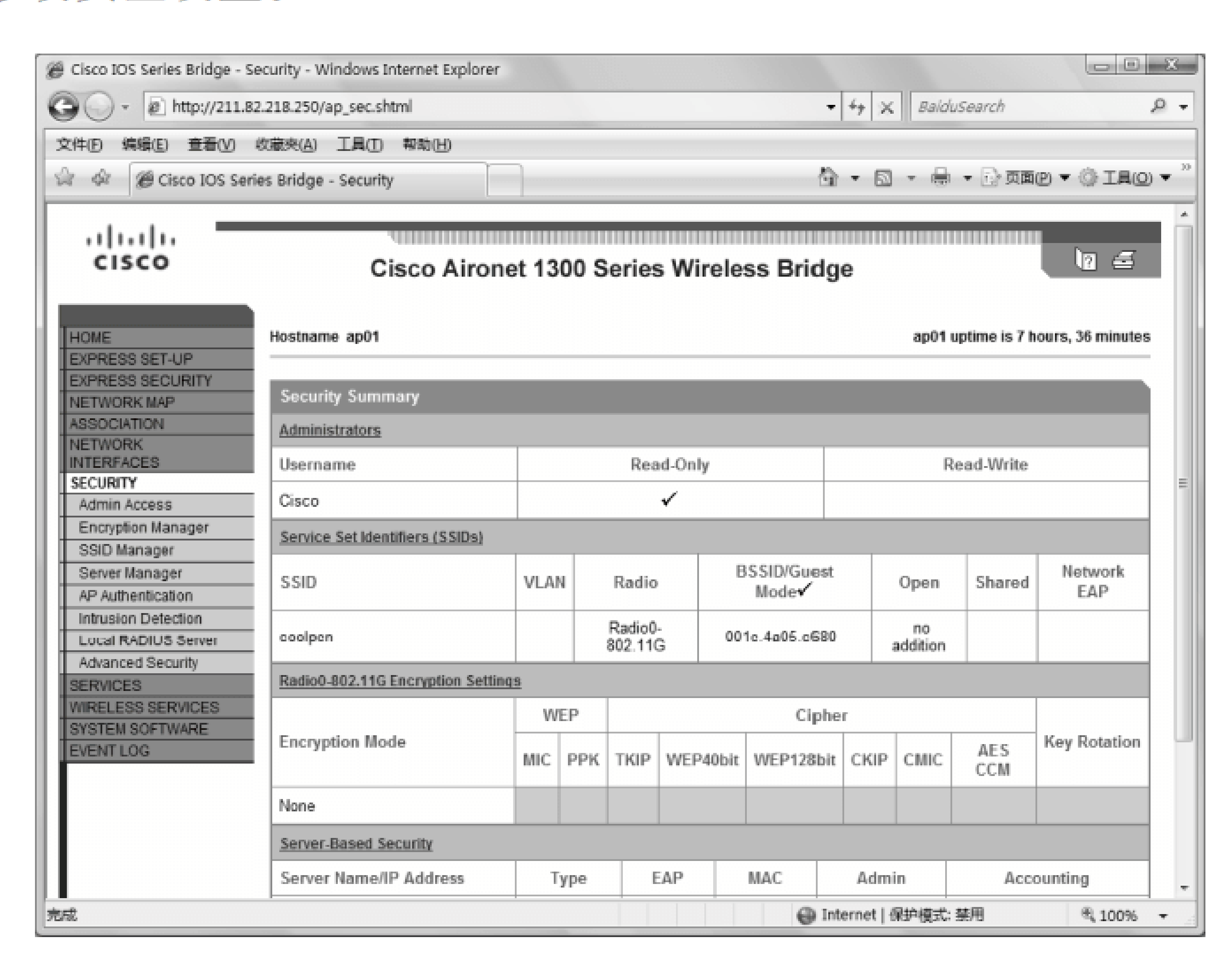


图 7-9 当前安全设置

(2) 在安全配置窗口中,单击左侧导航栏中的 SSID Manager,打开如图 7-10 所示的 Security: Global SSID Manager 窗口,在 SSID Properties 选项区域,选择 NEW 选项并在左侧设置新的 SSID 即可。

(3) 在如图 7-11 所示的 Client Authentication Settings 选项区域,可以设置客户端身份验证方法,首先选择希望使用的验证方法,选中 Open Authentication 复选框,并在后面的下拉列表框中选择具体验证方式即可,包括 MAC 地址、EAP 加密等。然后,在 Server Priorities(服务器优先级)选项区域,选择所设置不同验证方式的执行顺序(必须同时使用多种验证方式才可设置),通常情况下都是使用默认设置。

(4) 在如图 7-12 所示的 Client Authenticated Key Management 选项区域,可以设置客户端验证密钥的管理方式,包括 mandatory(强制执行)和 optional(任意选择)两种方式,如果选中 Enable WPA 复选框启用 WPA 加密功能,则还必须设置相应的加密密码。

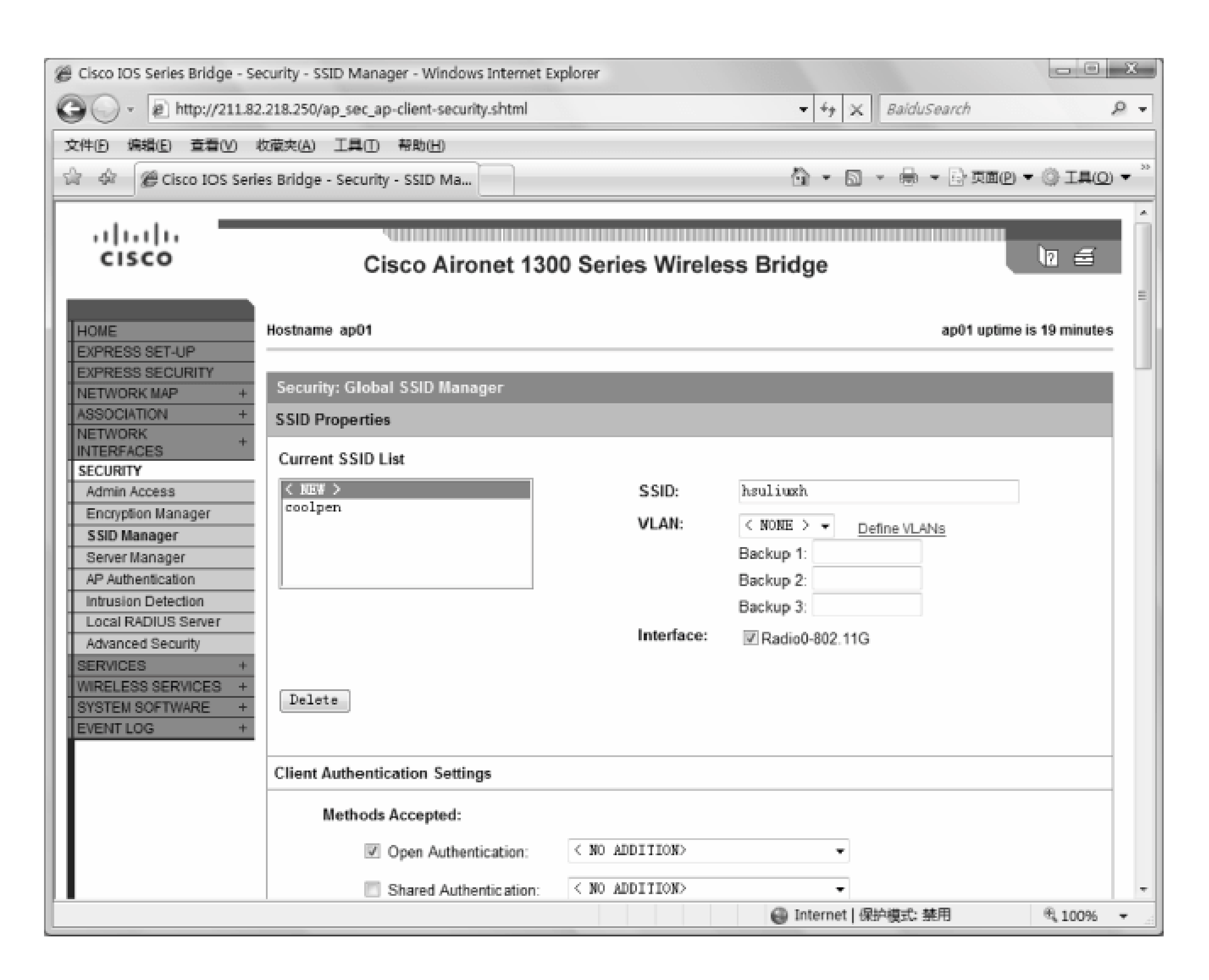


图 7-10 Security：Global SSID Manager 窗口

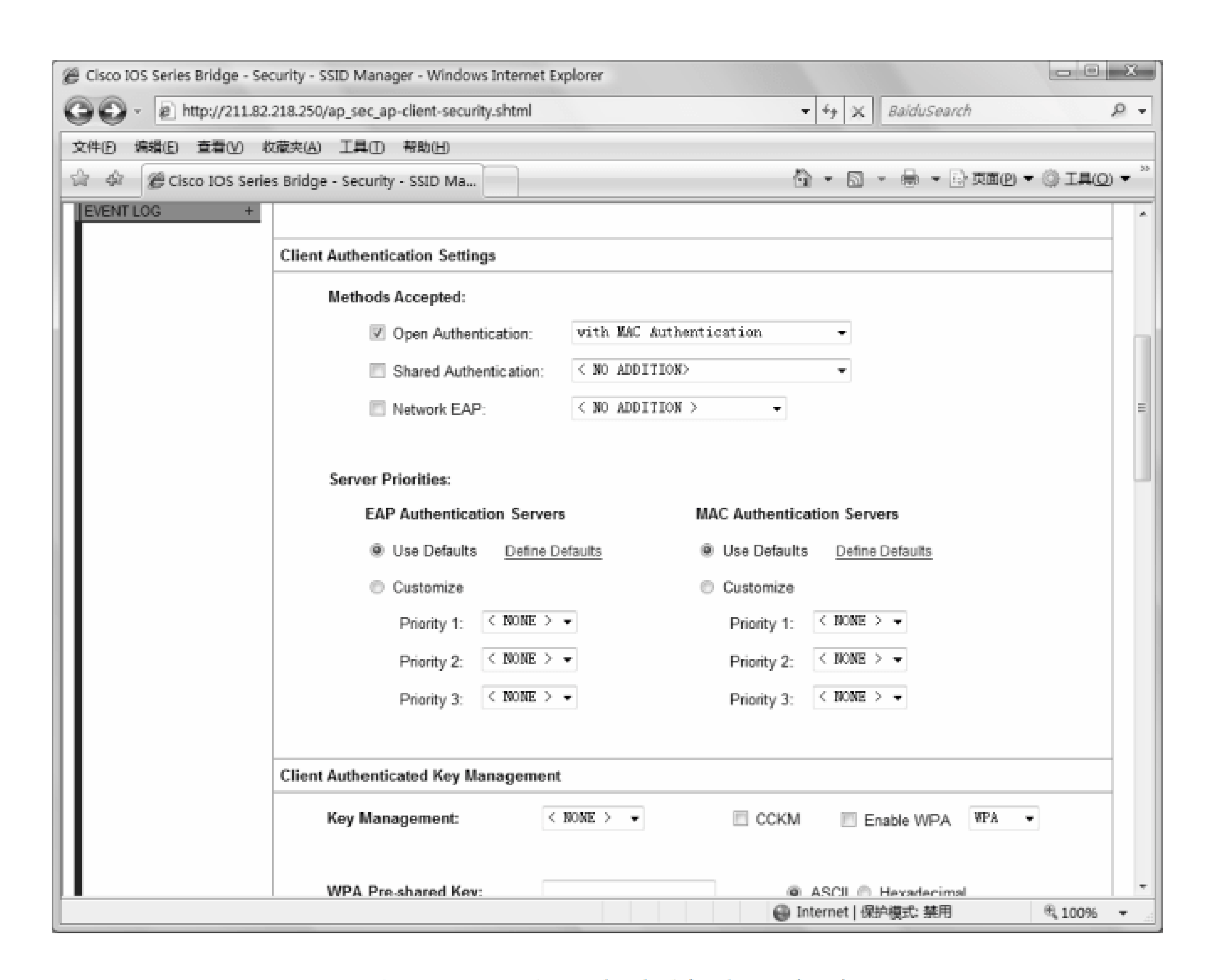


图 7-11 设置客户端验证方式

（5）在如图 7-13 所示的 Multiple BSSID Beacon Settings 选项区域，切记不要选中 Set SSID as Guest Mode 复选框，所谓的 BSSID 是 SSID 的一种，SSID 是对 BSSID 和 ESSID 的缩写和统称。如果在无线网络只有一个无线路由器或 AP 发射源时，则各个客户端使用统一的 BSSID 名称和 AP 通信；如果在无线网络有多个无线路由器或 AP 发射源并相互通过 WDS（Wireless Distribution System，无线分布式系统）等方式连接时，各个客户端使用统一的 ESSID 信息和 AP 通信。

（6）在 Guest Mode/Infrastructure SSID Settings 选项区域，选中 Single BSSID 单选按钮即可。选中 Multiple BSSID 单选按钮后，无线客户端可以通过设置自己的 SSID 加入 AP

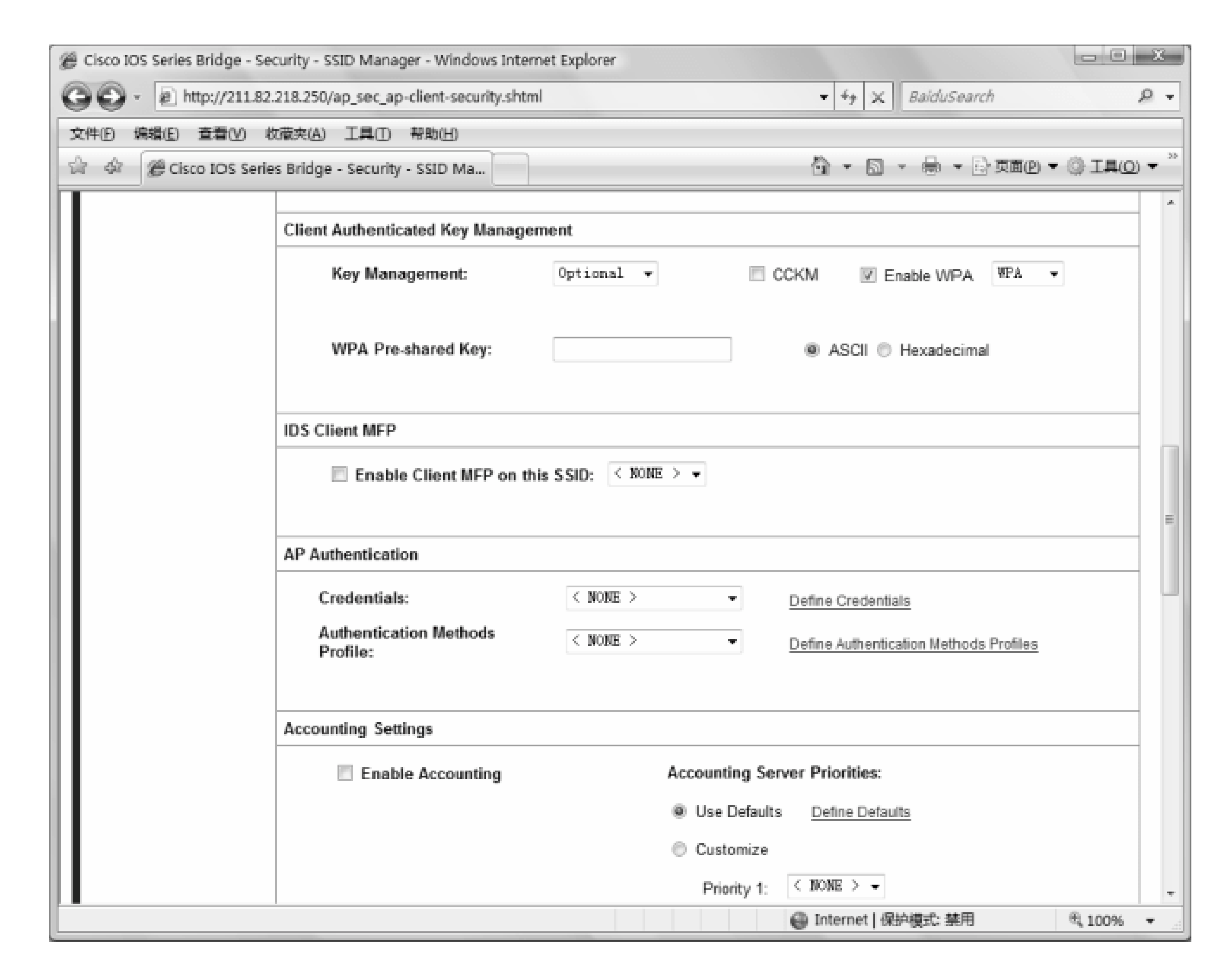


图 7-12　设置客户端验证密钥管理方式及其他

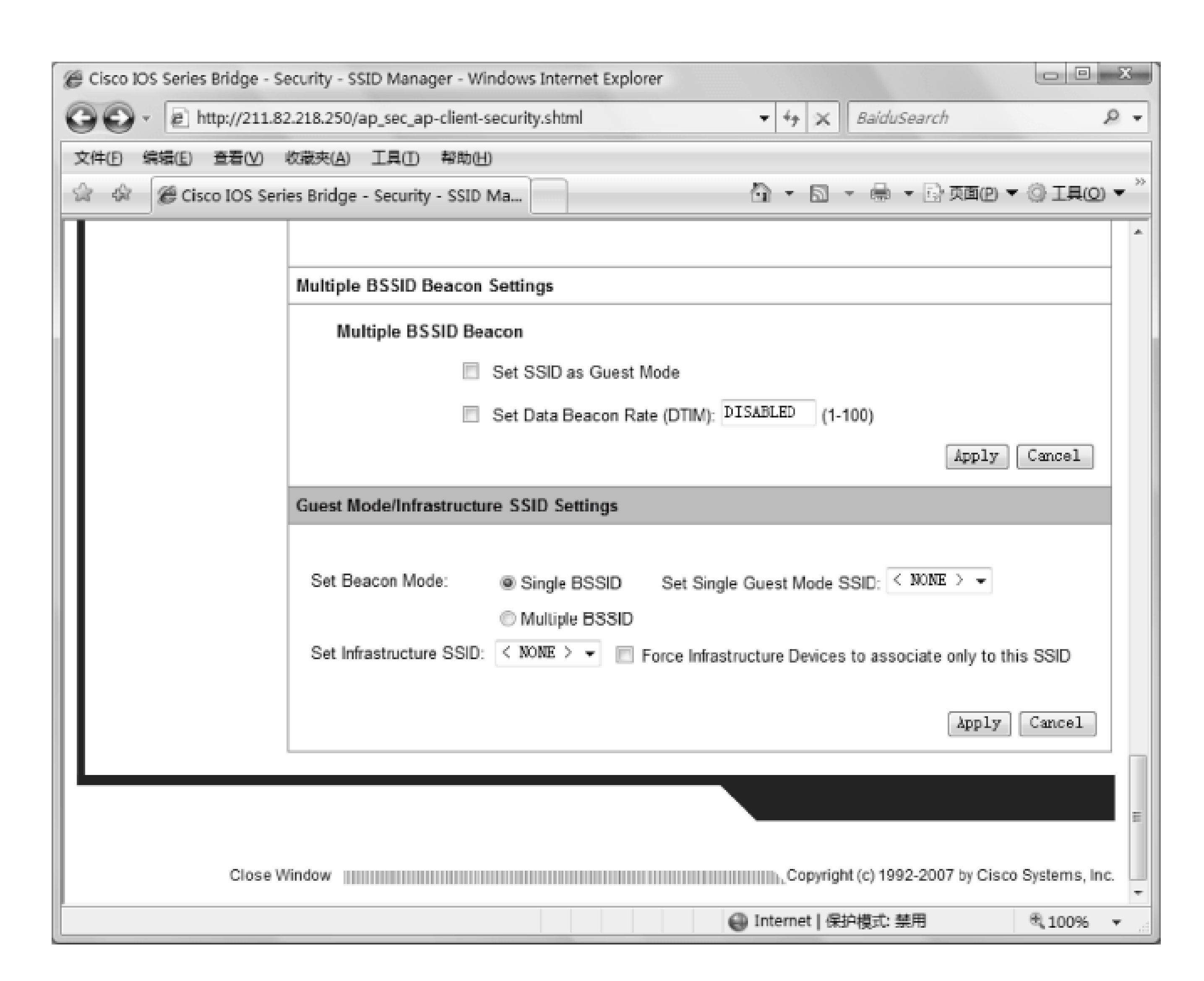


图 7-13　多重 BSSID 设置

划分的不同 VLAN 中,可以提高网络安全性,普通用户不推荐配置此功能。

(7) 取消无线 AP 的 SSID 广播也是非常重要的,在 Cisco Aironet 1300 无线网桥的 Web 配置窗口中,单击左侧导航栏中的 EXPRESS SECURITY,显示如图 7-14 所示的 Express Security Set-Up 窗口,确认 SSID 文本框后的 Broadcast SSID in Beacon 复选框未被选中,即可阻止无线 AP 在覆盖范围内广播自己的 SSID。

提示:修改无线 AP 的 SSID 后,也必须在工作站的无线网络属性中作相应的设置,从而保持与无线 AP 的一致。在无线漫游网络中,所有无线 AP 的 SSID 必须保持相同。

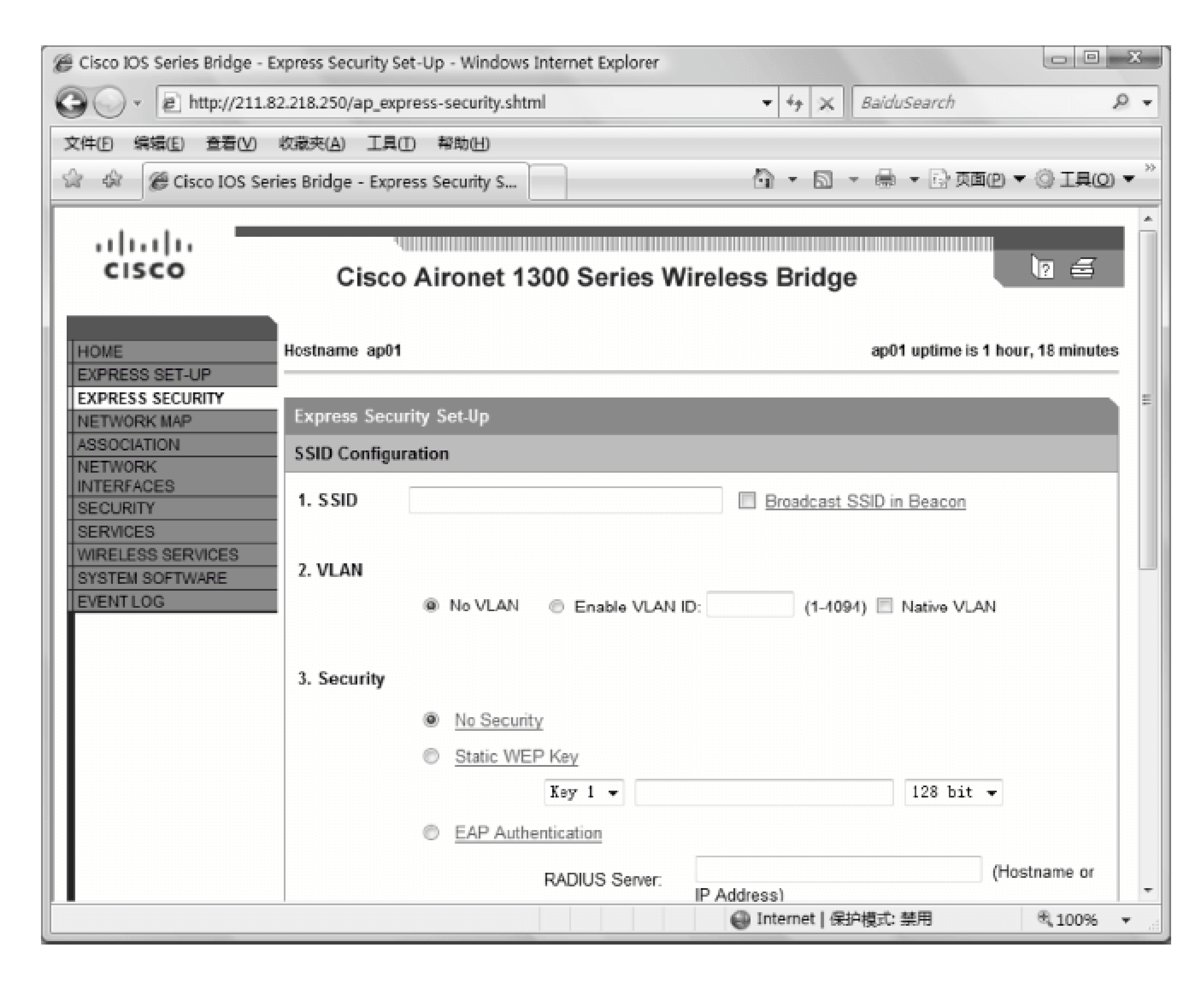


图 7-14 Express Security Set-Up 窗口

7.5.2 配置访问列表

配置 ACL 是 Cisco IOS 的功能之一。Cisco Aironet 1300 无线网桥允许用户配置多种访问列表，包括 MAC 地址访问控制列表、IP 访问列表和协议类型访问列表。

1. MAC 地址访问列表

在 Cisco Aironet 1300 的安全配置窗口中，依次展开 SERVICES→FITERS 选项，切换到如图 7-15 所示的 MAC ADDRESS FILTERS 选项卡，在 Create/Edit Filter Name 下拉菜单中，可以选择并编辑现有 MAC 访问列表，如果选择 NEW 选项，则可以新建 MAC 访问列表；在 Filter Index 文本框中，输入访问列表号，MAC 地址访问列表号的范围是 700～799；在 Add MAC Address 输入网络设备或端口的 MAC 地址，如果输入子网掩码则可以设置一段 MAC 地址；在 Action 下拉列表框中，执行的操作有 Forward 或 Block。切记，最后一定要设置 Default Action 选项，即默认操作。

2. IP 访问列表

在 Cisco Aironet 1300 的安全配置窗口中，依次展开 SERVICES→FITERS 选项，切换到如图 7-16 所示的 IP FILTERS 选项卡，在 Create/Edit Filter Name 下拉菜单中，可以选择并编辑现有 IP 访问列表，如果选择 NEW 选项，则可以新建 IP 访问列表。在 Filter Name 文本框中输入新建访问列表的名称，如 Office；在 Default Action 下拉列表框中选择默认的操作，Block All（阻止所有）或 Forward All（放行所有）；在 Destination Address 文本框中输入目标 IP 地址和子网掩码；在 Source Address 文本框中输入源 IP 地址和子网掩码；在 Action 下拉列表框中，执行的操作有 Forward 或 Block。最后，单击 Add 按钮，将其添加到 Filters Classes 列表中。IP Protocol 和 UDP/TCP Port 区域的设置与此类似，这里不再赘述。

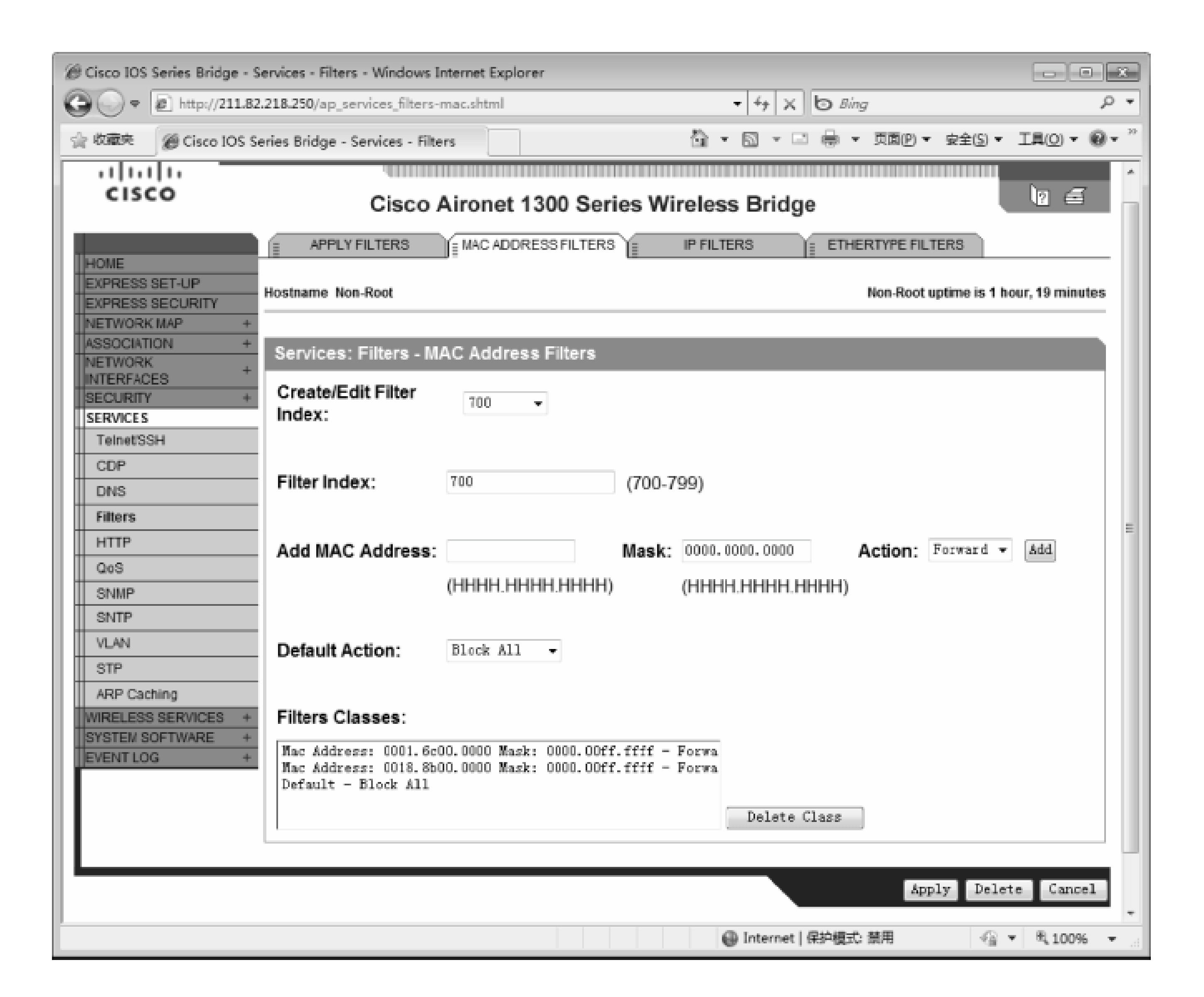


图 7-15 MAC ADDRESS FILTERS 选项卡

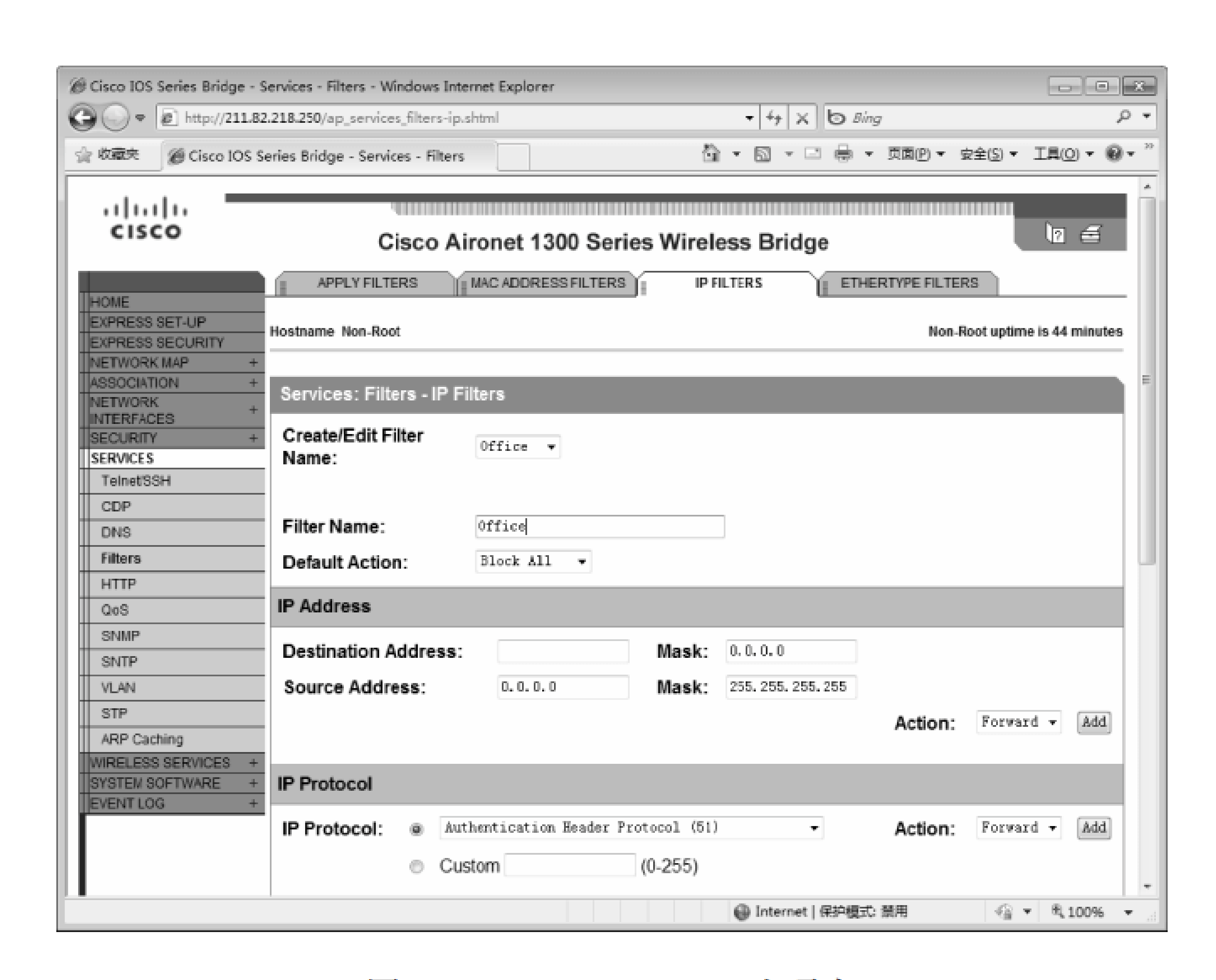


图 7-16 IP FILTERS 选项卡

7.5.3 配置 WEP 加密

IEEE 802.11 的安全性选项包括以 WEP 算法为基础的身份验证服务和加密服务。WEP 是一套安全服务，用来防止 IEEE 802.11 网络受到未授权用户的访问，例如偷听（捕获无线网络通信）等。利用自动无线网络配置，可以指定进入网络时用于身份验证的网络密钥。也可以指定使用哪个网络密码来对通过该网络传输的数据进行加密。启用数据加密时，生成秘密的共享加密密钥，因而避免泄露给偷听者。

1. 开放式系统和共享密钥身份验证

IEEE 802.11 支持两个子类型的网络身份验证服务，即开放式系统和共享密钥。在“开放式身份验证”下，任何无线站都可请求身份验证。需要通过一个身份验证的无线站将包含发送站的身份验证管理帧发送出去。接收站然后将表明其是否识别发送站的身份的帧发送回去。在“共享密钥”身份验证下，每个无线站都被假定为具有安全频道的秘密共享密钥，该安全频道独立于 IEEE 802.11 无线网络通信频道。要使用“共享密钥”身份验证，必须具有一个网络密钥。

2. 网络密钥

启用 WEP 时，用户可以指定用于加密的网络密钥。可为用户自动提供网络密钥（例如，可能会提供在无线网络适配器上），用户也可以通过输入方式来亲自指定密钥。如果用户亲自指定密钥，还可以指定密钥长度（40 位或 104 位）、密钥格式（ASCII 字符或十六进制数字）和密钥索引（存储特定密钥的位置）。密钥长度越长，密钥越安全。密钥长度每增加一位，可能的密钥数量就会增加一倍。

在 IEEE 802.11 下，可用多达 4 个密钥（密钥索引值为 0、1、2 和 3）配置无线站。当访问点或无线站利用存储在特定密钥索引中的密钥传送加密邮件时，传送的邮件指明用来对邮件正文加密的密钥索引。然后接收访问点或无线站可以检索存储在密钥索引处的密码并使用它来对加密邮件正文进行解码。

以 Cisco Aironet 1300 无线网桥为例，在安全配置窗口中，单击导航栏中的 Encryption Manager，打开如图 7-17 所示的 Security：Encryption Manager 窗口。系统默认选中 None 单选按钮，即为启用加密功能。在 Encryption Modes 选项区域选中 WEP Encryption 或 Cipher 单选按钮，即可启用 WEP 加密或使用其他加密方法。Cisco Aironet 1300 无线网桥支持 WEP、TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议）、CMIC（Cisco Message Integrity Check，思科消息完整性检测）等多种加密协议，或者多种协议配合使用

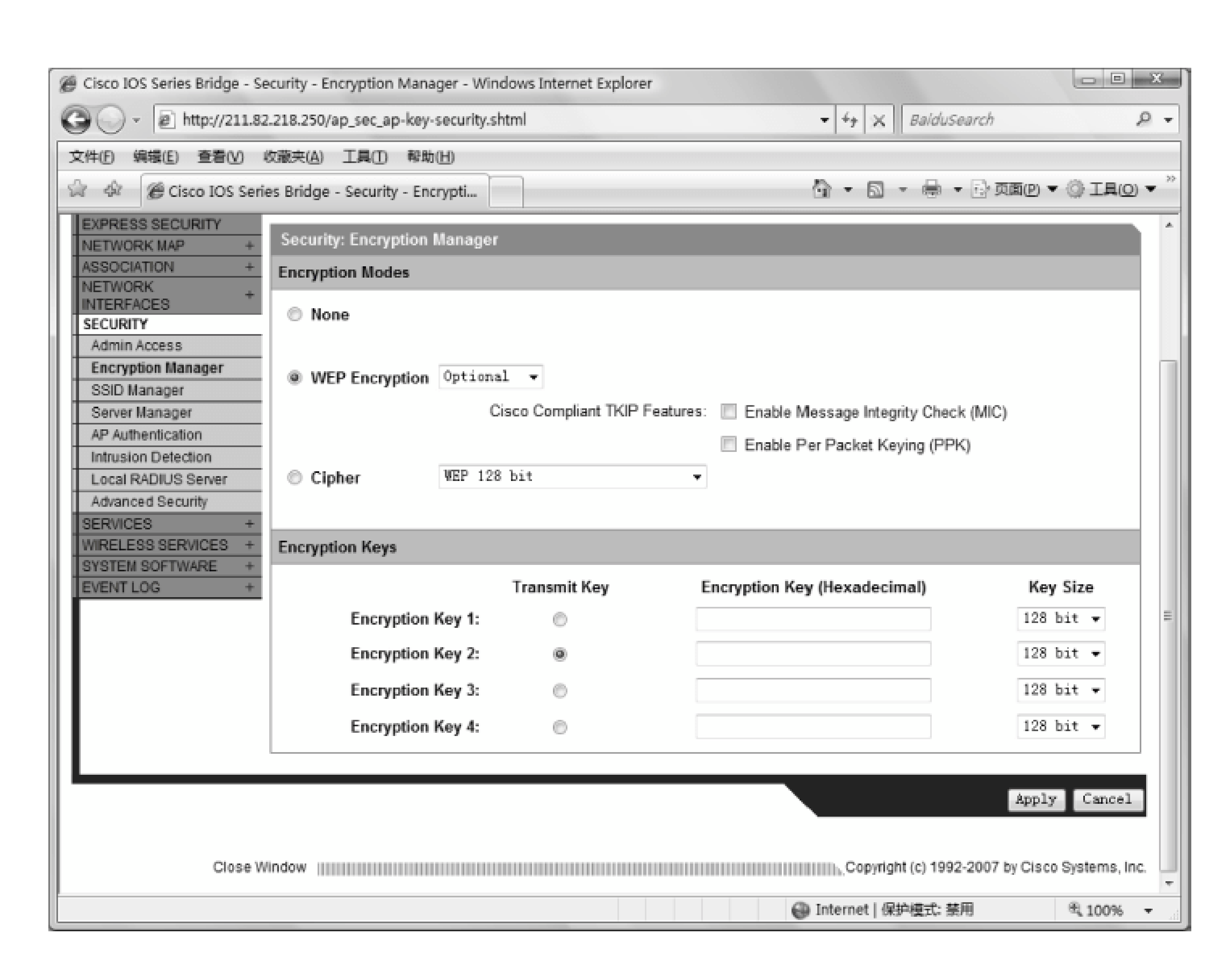


图 7-17　启用 WEP 加密

加强安全性。在 Encryption Keys 选项区域，分别设置相应的 Encryption Key 值即可。需要注意的是，密钥越长，加密效果越好，但同时也将占用更多的性能，从而导致无线传输速率下降。

7.5.4 配置入侵检测功能

有些无线 AP 本身已经集成了简单的入侵检测功能，可以帮助网络管理员保护管理端口，在第一时间识别各种网络入侵。需要注意的是，启用该功能后，可能影响到设备 QoS，因此建议普通用户保持默认设置，即不启用该功能。

在 Cisco Aironet 1300 无线网桥的安全配置窗口中，单击左侧导航栏中的 Intrusion Detection，打开如图 7-18 所示的 Intrusion Detection：Management Frame Protection 窗口。如果选中 Transmit MFP Frames 复选框，则该 AP 向外发送信息时将自动对信息完整性进行保护和验证，同时要求接收端必须是当前 WDS 中的成员，否则将无法成功阅读消息。如果选中 Detect MFP Frames 复选框，则无线 AP 将对每一个传入连接进行验证，确保消息的完整性和有效性，抵御外来侵袭。

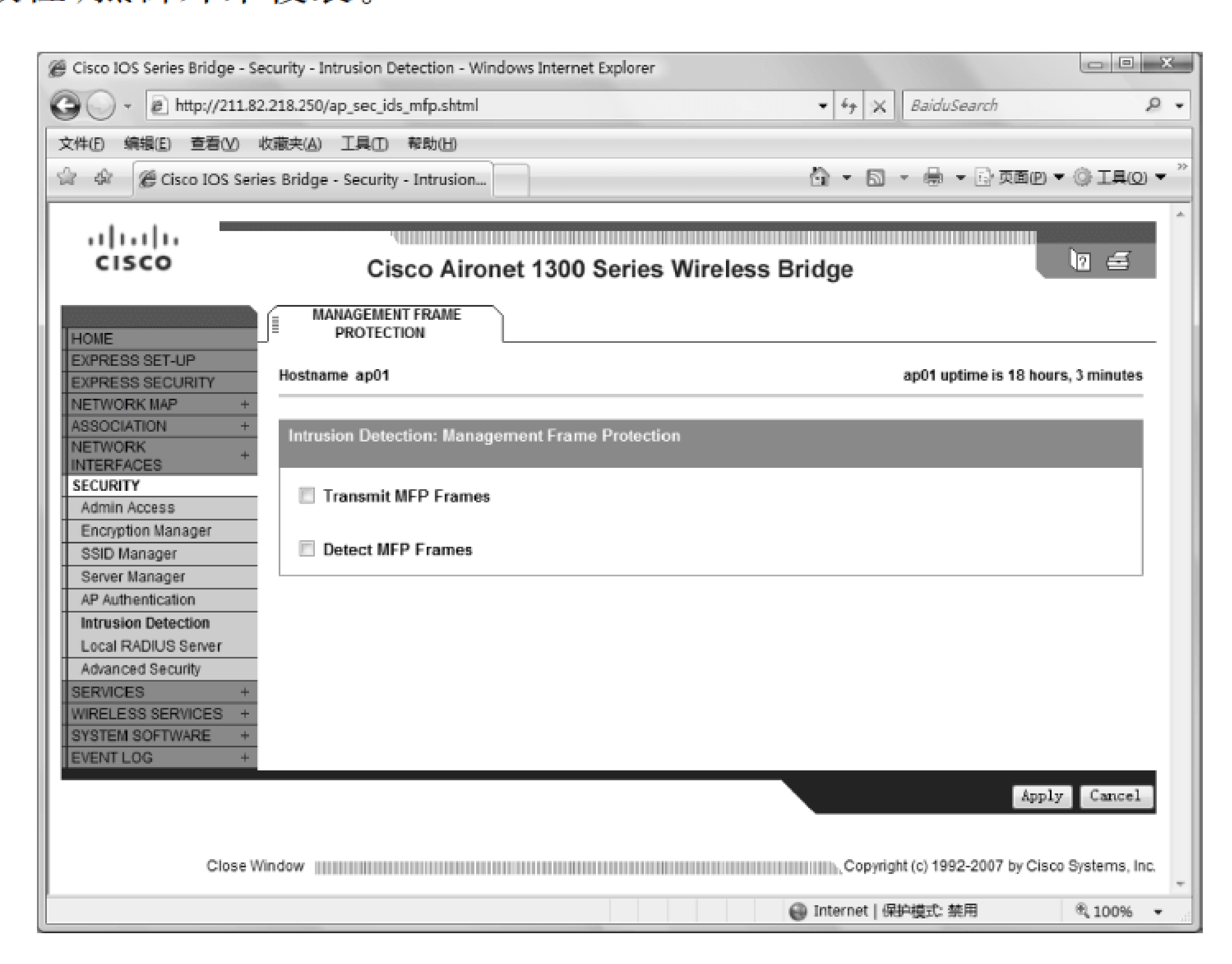


图 7-18 Intrusion Detection：Management Frame Protection 窗口

习题

1. 三层交换机通常可以支持哪些基本安全配置？各有什么作用？
2. 简述如何配置核心交换机的端口流量分析。
3. 什么是访问列表？有哪几种类型？
4. 简述无线网络中 SSID 的作用，如何通过配置 SSID 保护无线网络安全。
5. 什么是 NAT 接入技术？有哪几种实现方式？

实验：为无线 AP 配置并应用访问列表

实验目的：

掌握访问列表在网络安全中的应用。

实验内容：

根据无线客户端计算机的 MAC 地址，配置 MAC 地址访问列表，只允许列表中的计算机通过无线 AP 接入企业网络。

实验步骤：

（1）获取所有允许连接无线 AP 的计算机的 MAC 地址，可以通过 ipconfig 命令或 MAC 地址扫描工具实现。

（2）编辑 MAC 地址访问列表。

（3）将访问列表条目应用到无线 AP 的以太网口，并保存配置。

（4）使用一台列表中未包括的计算机访问无线 AP，验证配置效果。

第 8 章 chapter 8

局域网接入安全认证

局域网中包含的网络设备复杂多样，比较常用的设备包括路由器、交换机、防火墙、无线AP、服务器等。随着IEEE 802.11无线局域网和普遍宽带互联网连接的广泛部署，安全问题不仅存在于网络外围，还存在于网络内部，网络设备的安全接入和访问控制已经成了网络安全的一部分。能够防御这些安全漏洞的身份识别网络技术现已成为吸引全球客户关注的主要技术。

8.1 局域网接入安全认证规划

在企业网络中，局域网接入安全认证系统对网络安全起着非常重要的作用，不仅能够杜绝非法终端随意接入网络，而且可以为通过安全认证的终端设备获得相应的访问权限。该企业局域网中的大部分网络设备均支持802.1x认证机制，通过为展示厅、办公区等开放性较高的区域的网络设备启用安全认证功能，可以阻止危险因素的入侵。

8.1.1 案例情景

目前，在该企业网络中没有任何终端接入安全认证系统，任何品牌、型号的交换机、计算机、防火墙等网络设备都可以随意接入网络。在展示厅部署的无线局域网系统，所有无线客户端均可以通过无线AP接入企业局域网，并通过局域网接入Internet。如果临时接入网络的客户端计算机存在安全隐患，则将直接影响局域网的安全。在办公区如果企业员工将私人计算机带到单位，并接入局域网，则很容易造成企业机密信息外泄。

该网络中缺乏集中的报告和监控系统，一旦出现问题，管理员只能调出近期所有的网络日志信息，由于日志信息量的庞大，管理员的工作负担是可想而知的。

8.1.2 项目需求

大量的网络安全事件证明，网络内部的不安全因素远比外网入侵严重。堵住内网安全漏洞才是打造企业安全稳定局域网的重要因素。为了提供局域网接入的安全性，需要对终端设备的身份进行集中认证管理，对网络设备进行统一管理，提高局域网接入的灵活性、安全性和移动性，进一步增强网络访问安全。通过身份验证机制对客户端执行不同的访问策略，严格限制网络终端的访问行为。为了减轻管理员的工作负担，需要在网络中部署局域网接入记账系统，实时记录终端设备的接入情况。

802.1x 是目前比较常用的身份验证方法之一。该企业网络中有几十个用户，每个用户接入到网络中都需要身份验证。如果在路由器上通过命令实现，不仅工作量大，而且容易出错。此时就需要在网络中部署 ACS 服务器，用于处理网络设备发送过来的客户端身份验证请求，并根据用户策略授予用户不同的访问权限。另外，ACS 服务器还可以把用户的访问记录从开始到结束，全部记录下来，然后管理员可以随时查看处理这些问题。

8.1.3　解决方案

通过在企业网络中部署 ACS 服务器，可以对接入局域网的终端设备进行集中身份验证、记账，避免存在安全隐患的网络设备接入网络。CiscoSecure ACS 是一款由 Cisco 公司分发和维护的访问控制和记账系统。CiscoSecure ACS 服务器是具高可扩展性的高性能访问控制服务器，可作为集中的 RADIUS 服务器运行。CiscoSecure ACS 将验证、企业员工访问和管理员访问与策略控制结合在一个集中的身份识别网络解决方案中。它通过对所有企业员工账户使用一个集中数据库，CiscoSecure ACS 可集中控制所有的员工权限并将他们分配到网络中的几百甚至几千个接入点。

对于记账服务，CiscoSecure ACS 针对员工的网络行为提供具体的报告和监控功能，并记录整个网络上每次的访问连接和设备配置变化。CiscoSecure ACS 支持广泛的访问连接，包括有线和无线局域网、宽带、内容、存储、IP 上的语音(VoIP)、防火墙和 VPN 等。

8.2　安装和配置 ACS 服务器

CiscoSecure ACS 是 Cisco IBNS(Identity Based Networking Services，基于身份的网络服务)架构的重要组件。Cisco IBNS 基于 802.1x 和 EAP 等端口安全标准，并将安全验证、授权和记账(AAA)从网络外围扩展到了局域网中的每个连接点。用户可在这个全新架构中部署新的策略控制工具(如每个用户的配额、VLAN 分配和 ACL)，这是因为思科交换机和无线接入点的扩展功能可用于在 RADIUS 协议上查询 CiscoSecure ACS。

8.2.1　安装 Java 虚拟机

严格地讲，Java 虚拟机环境并不是 ACS 服务器的必需组件，而是为远程管理 ACS 服务器准备的。如果需要在远程计算机上管理 ACS 服务器，则 ACS 服务器和远程管理计算机上必须同时安装 Java 虚拟机，如图 8-1 所示。Sun Java 虚拟机的下载地址如下：



图 8-1　安装 Java 虚拟机

http://www.javaresearch.org/members/jross/jdk/jdk-1_5_0-windows-i586.exe

8.2.2　安装 ACS 服务器

完成所有准备工作之后，即可开始安装 CiscoSecure ACS 4.2，安装过程非常简单。在安装向导的帮助下，即可顺利完成。

（1）启动 CiscoSecure ACS 4.2 安装向导，显示 CiscoSecure ACS v4.2 Setup 对话框，单击 ACCEPT 按钮显示 Welcome 对话框，连续单击 Next 按钮，直至显示如图 8-2 所示的 Before You Begin 对话框，选中所有复选框方可继续进行。

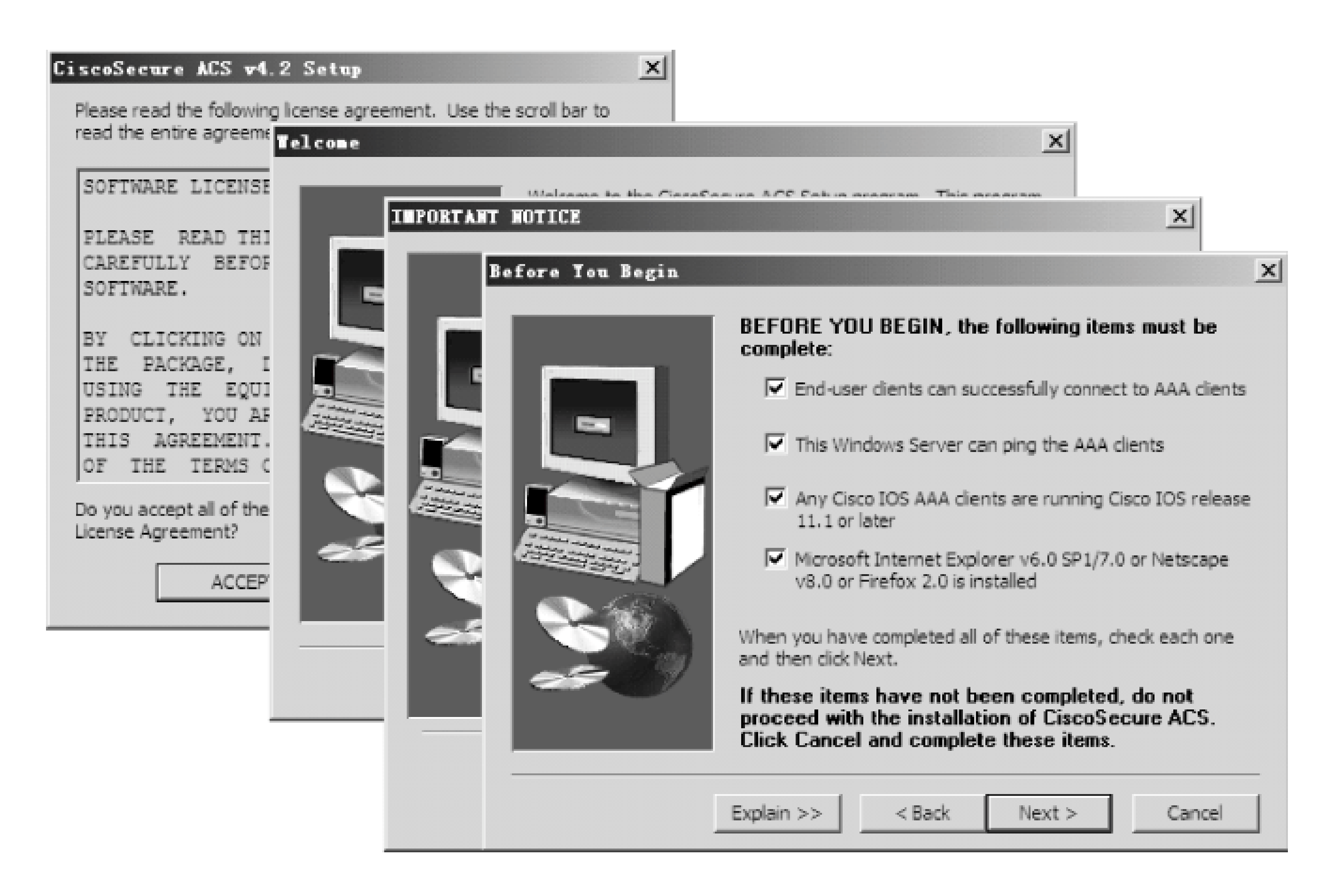


图 8-2 Before You Begin 对话框

（2）单击 Next 按钮，显示 Choose Destination Location 对话框，设置 ACS 的安装路径。单击 Next 按钮，显示 Authentication Database Configuration 对话框，选中 Check the ACS Internal Database only 单选按钮，单击 Next 按钮，显示 Advanced Options 对话框，在这里可以设置用户优先级，组优先组、最大支持的会话连接等内容，如图 8-3 所示。

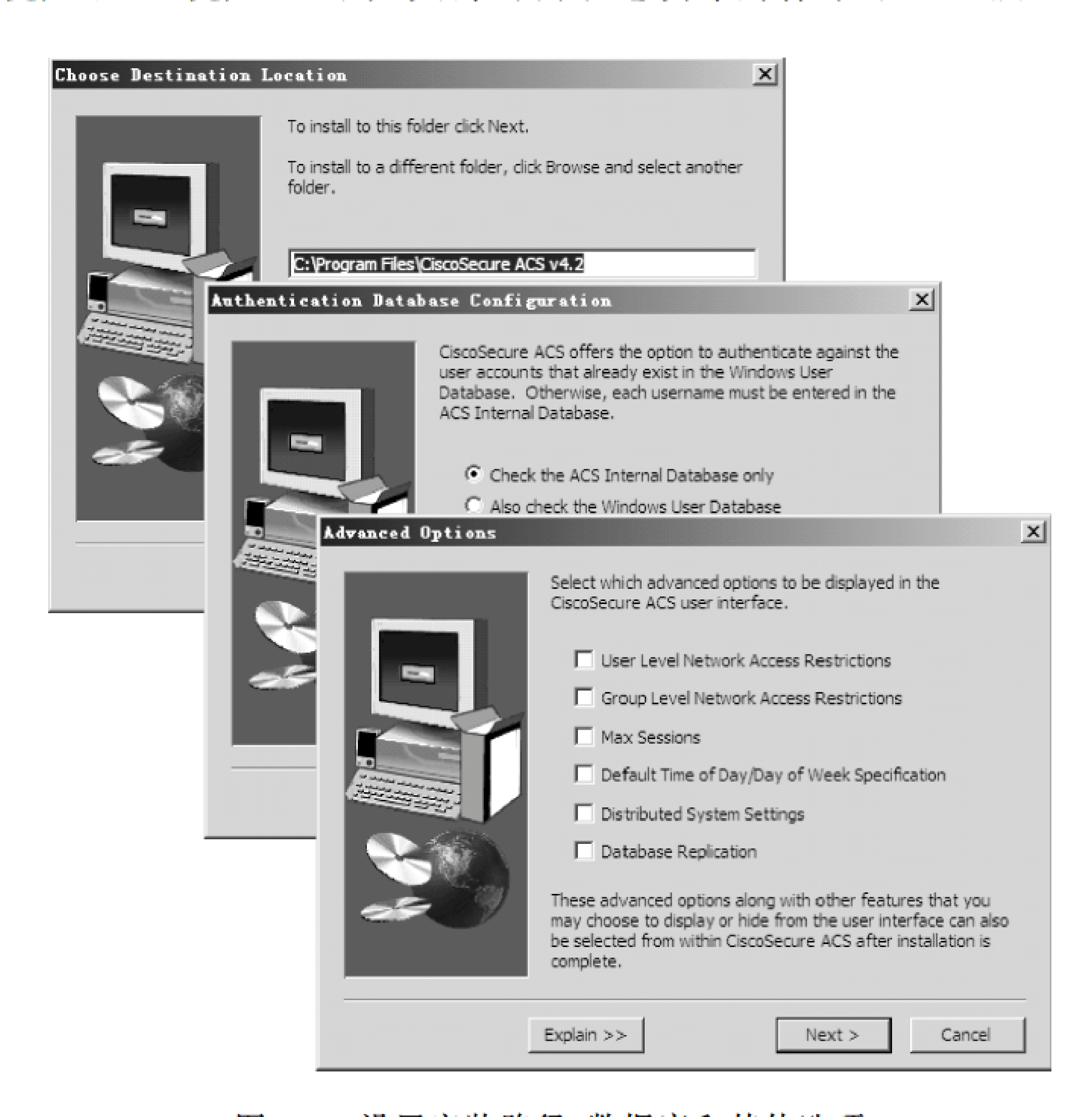


图 8-3 设置安装路径、数据库和其他选项

（3）单击 Next 按钮，显示如图 8-4 所示的 Active Service Monitoring 对话框，如果希望使用 ACS 服务器监听用户认证服务，则选中 Enable Log-in Monitoring 复选框，在 Script to execute 下拉列表框中选择 * Restart All 选项，即一旦 ACS 监听用户认证服务失败，立刻执行重启所有的 ACS 的服务，保证 ACS 正常提供服务。如果希望当系统监听到事件时 ACS 发送邮件信息，选中 Enable Mail Notifications 复选框，再输入相关的信息即可。

（4）单击 Next 按钮，显示如图 8-5 所示的 CiscoSecure ACS Service Initiation 对话框，设置数据库加密密码，当出现严重的问题需要手动访问 ACS 数据库时使用，一般不常用。密码长度最少 8 位字符，并且是字母和数字的组合。单击 Next 按钮，开始安装，完成后将提示是否立即启动 ACS。继续单击 Next 按钮完成安装。



图 8-4　Active Service Monitoring 对话框

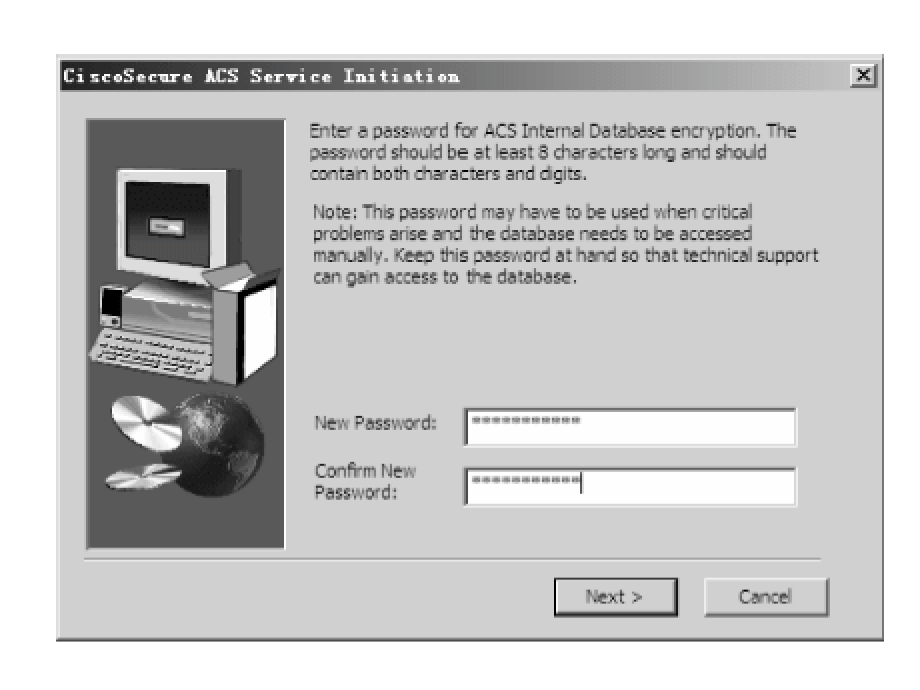


图 8-5　CiscoSecure ACS Service Initiation 对话框

（5）单击 Finish 按钮，结束安装，立即启动 ACS，显示如图 8-6 所示的 CiscoSecure ACS 窗口。

默认情况下，由于 IE 浏览器的默认安全级别较高，可能会阻止窗口内容的显示。此时，可以单击“工具”菜单，选择下拉菜单中的“Internet 选项”命令，显示“Internet 选项”对话框；切换到“安全”选项卡，选中“本地 Intranet”并单击“站点”按钮，显示“本地 Intranet”对话框。在“将该网站添加到区域”文本框中输入 ACS 服务器站点的地址，单击“添加”按钮添加到“网站”列表中，如图 8-7 所示。

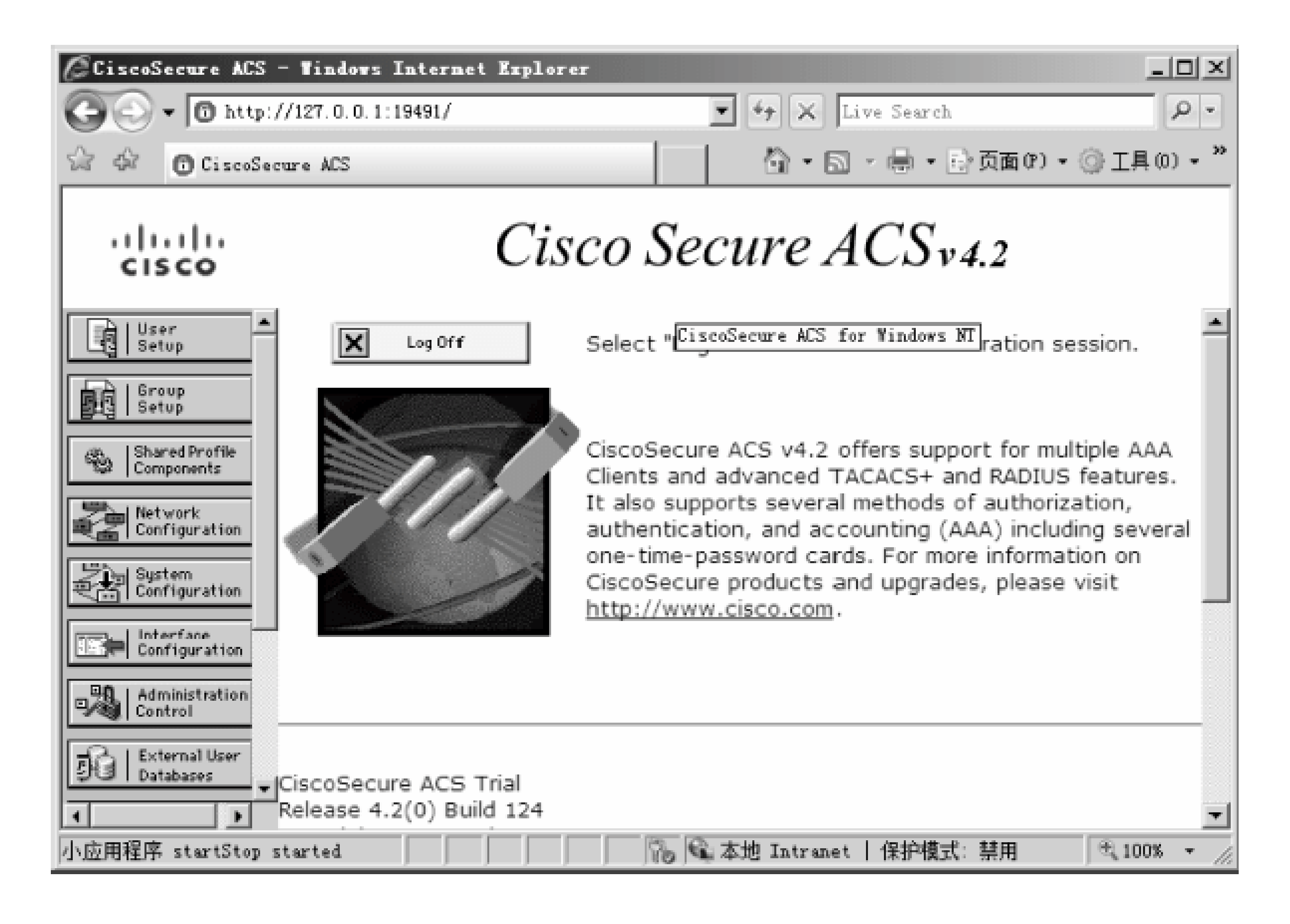


图 8-6　CiscoSecure ACS 窗口



图 8-7　调整 IE 浏览器安全级别

8.2.3 ACS 服务器基本配置

ACS 服务器安装完成之后，还必须进行配置才能与 Active Directory 协同工作，为 ACS 客户端提供审核和认证。

1. 配置加密算法

在 ACS 管理窗口中，依次单击 System Configuration→Global Authentication Setup 链接，显示如图 8-8 所示的 Global Authentication Setup 窗口。在 EAP Configuration 选项区域内选中 Allow EAP-MSCHAPv2 和 Allow EAP-GTC 复选框。在 MS-CHAP Authentication 选项区域内选中 Allow MS-CHAP Version 1 Authentication 和 Allow MS-CHAP Version 2 Authentication 复选框。单击 Submit+Restart 按钮，保存设置。

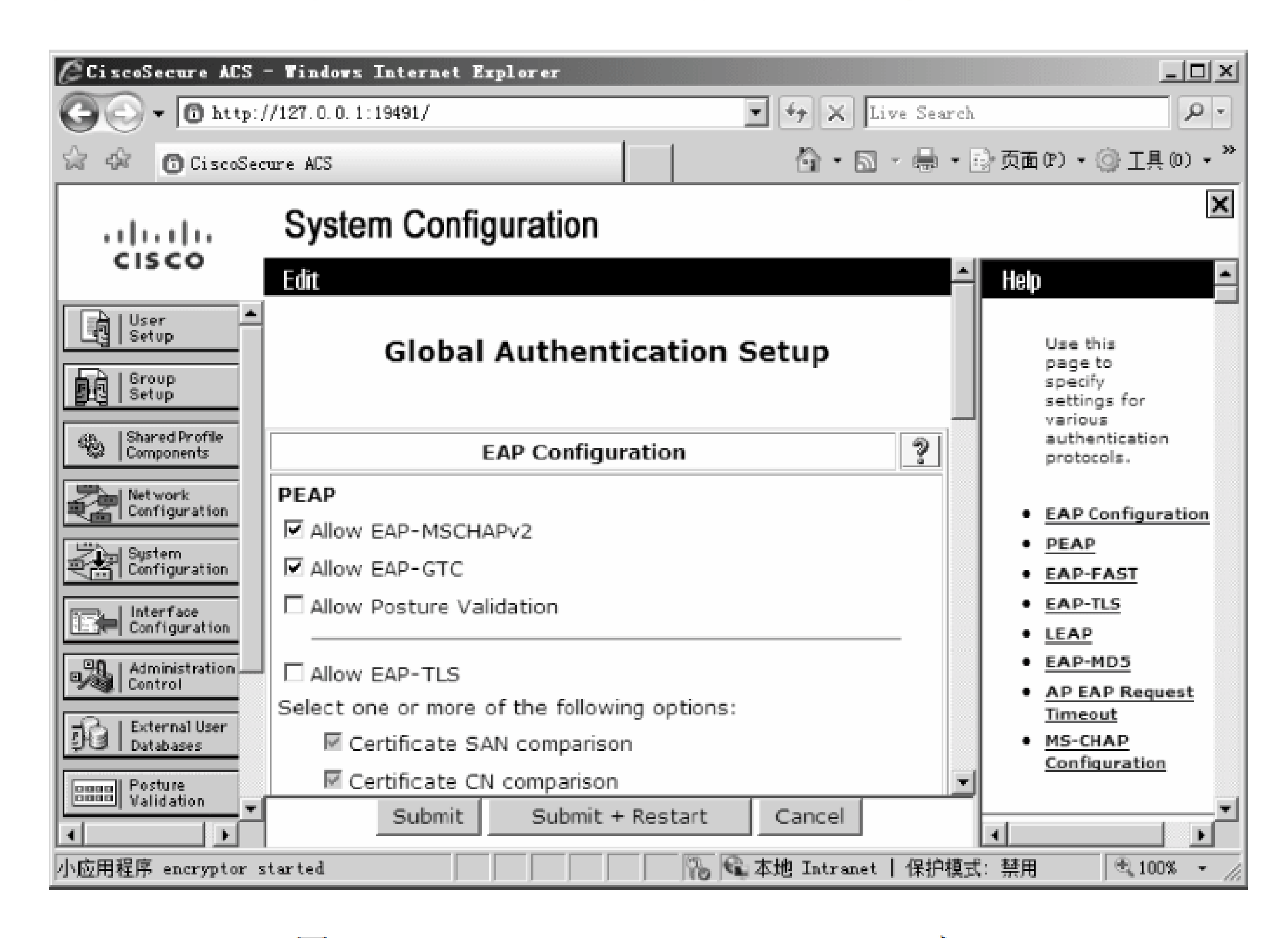


图 8-8 Global Authentication Setup 窗口

2. 配置 AAA Client

由于 ACS 客户端是无须任何代理组件的，所以管理员必须先在 ACS 服务器上配置 AAA Client。在 ACS 管理窗口中，单击 Network Configuration 按钮，显示 Network Configuration 窗口，在 AAA Client 选项区域内单击 Add Entry 按钮，显示如图 8-9 所示的 Add AAA Client 窗口。在 AAA Client Hostname 文本框中，输入配置 802.1x 身份验证功能的网络设备主机名；在 AAA Client IP Address 文本框中，输入网络设备的 IP 地址。在 Authenticate Using 下拉列表框中选择 RADIUS(Cisco IOS/PIX 6.0)选项。最后，单击 Submit+Apply 按钮保存设置。

3. 自定义授权命令集

通过自定义命令集，可以使 ACS 服务器仅对指定的命令进行授权和记账，即当用户登录网络设备运行授权的命令时可以执行，而运行未经授权的命令或子命令都是不允许的。

(1) 在 ACS 服务器管理窗口中，单击 Shared Profile Components 按钮，显示 Shared Profile Components 窗口，单击 Shell Command Authorization Sets 链接，显示如图 8-10 所示的窗口。

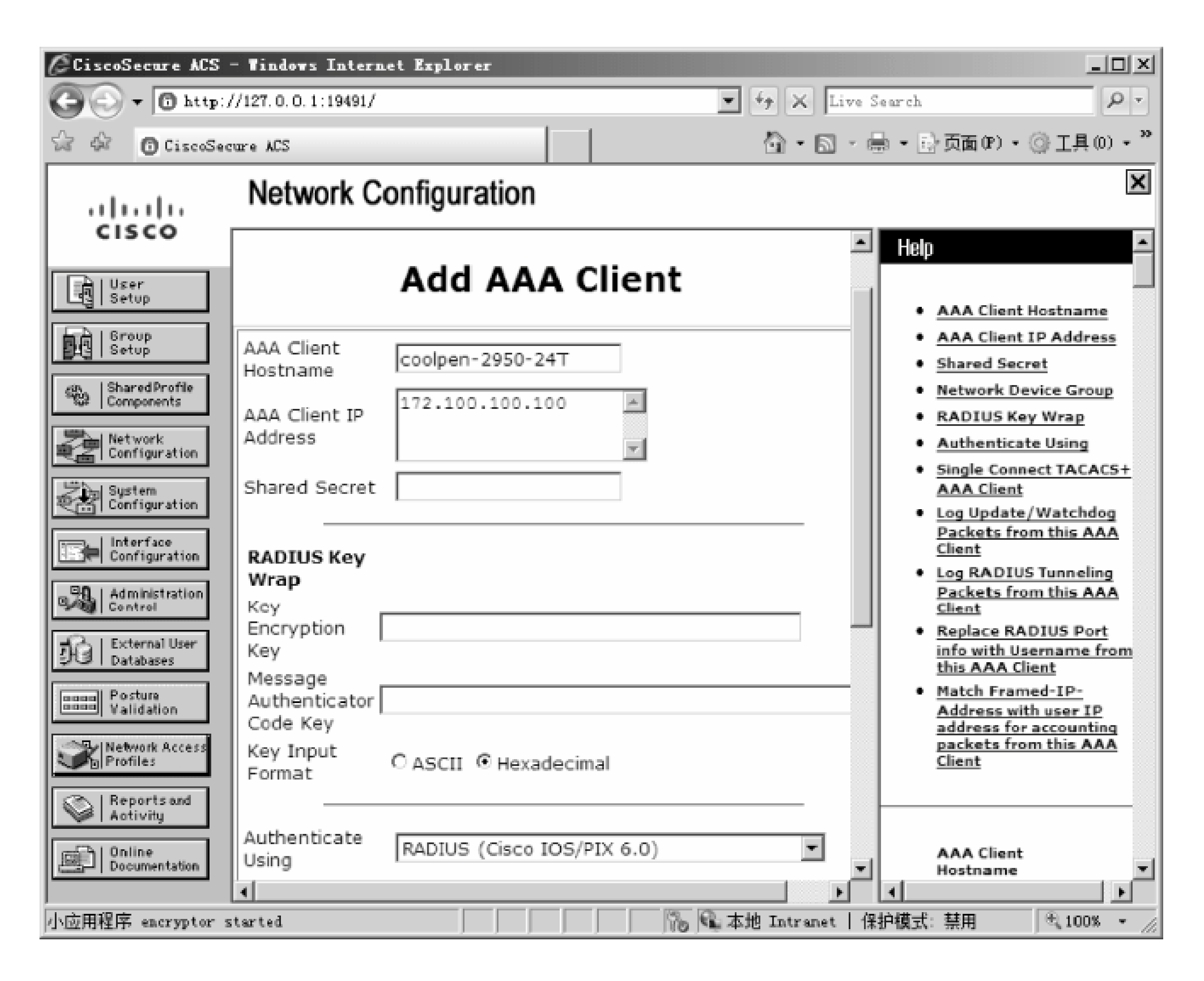


图 8-9　Add AAA Client 窗口

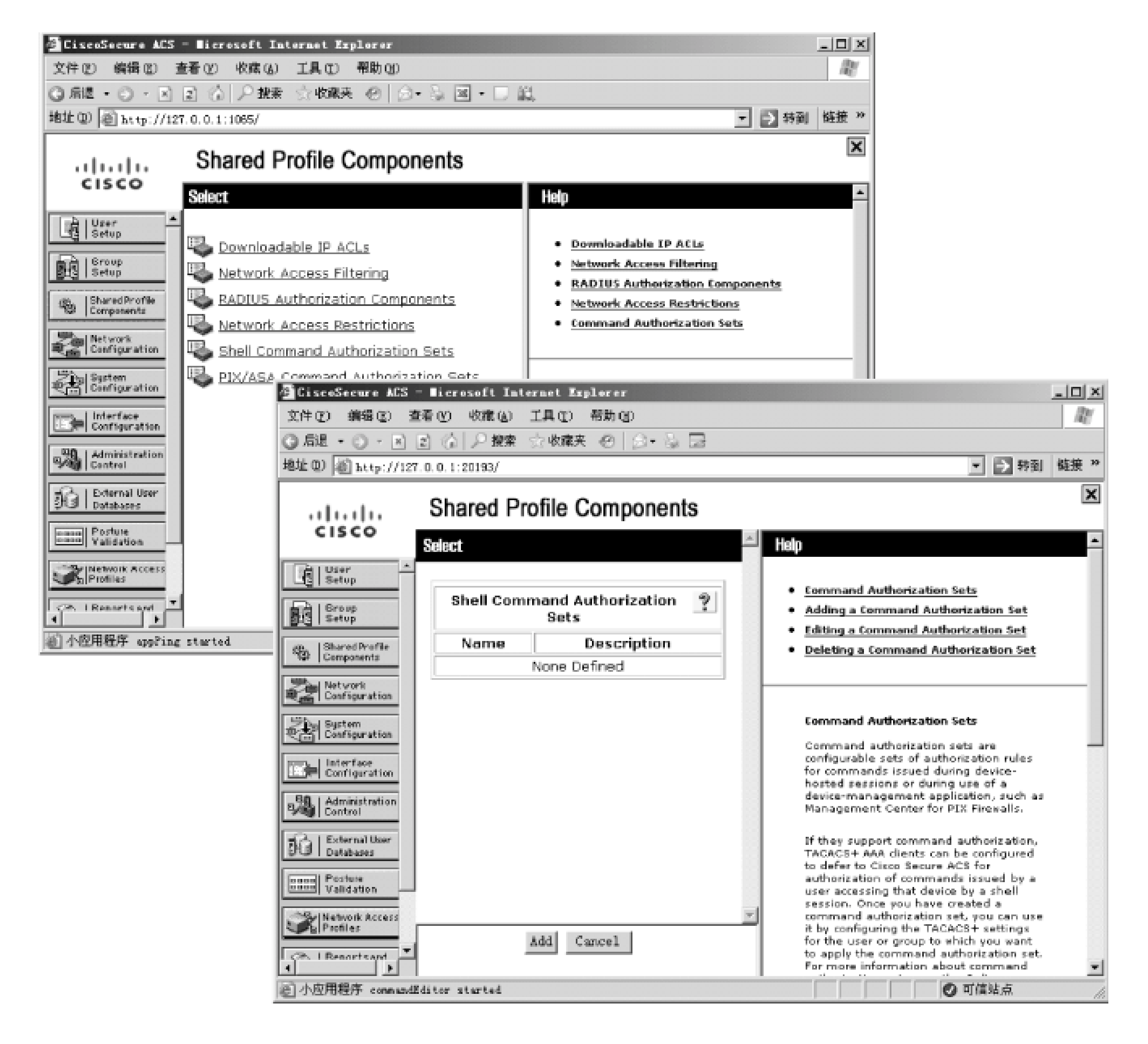


图 8-10　添加自定义授权命令集

(2) 单击 Add 按钮，显示如图 8-11 所示的 Shell Command Authorization Set 窗口。在 Name 文本框中输入命令集名称，例如 list。在 Description 文本框中输入命令集的描述信息。通过选中 Permit 或 Deny 单选按钮，可以允许或禁止对 Unmatched Commands 列表中指定的命令授权或记账，此处保留系统默认的 Deny 单选按钮。

(3) 在 Add Command 按钮上方的文本框中输入希望添加的命令，例如 configure，单击 Add Command 按钮，将其添加到上方的列表中，选中左侧列表中的命令，在右侧列表中直接

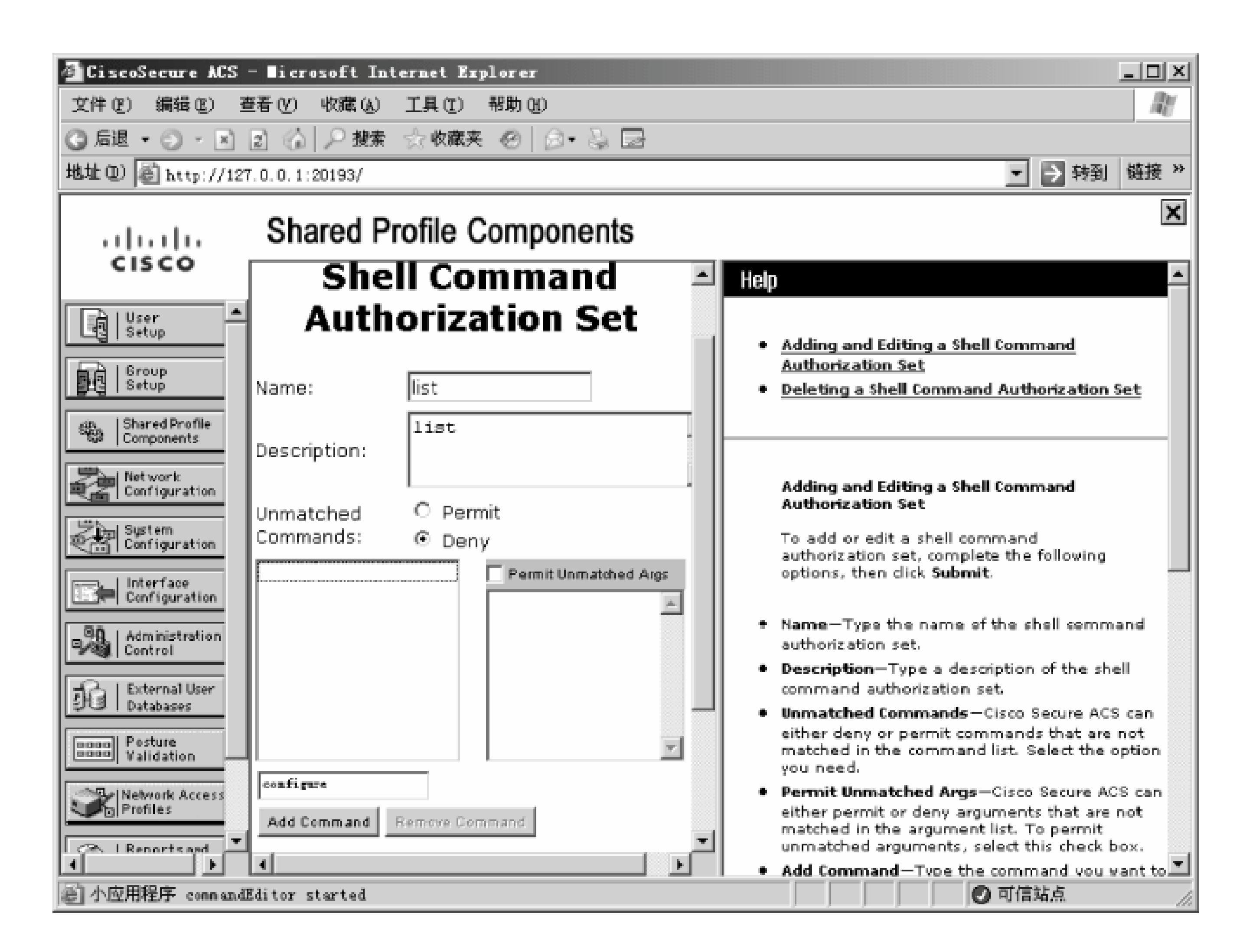


图 8-11 Shell Command Authorization Set 窗口

输入与其相关的参数，格式为“permit＋参数”，例如 permit terminal。ACS 服务器可以允许或拒绝右侧参数列表中不匹配的参数，建议选中 Permit Unmatched Args 复选框，如图 8-12 所示。

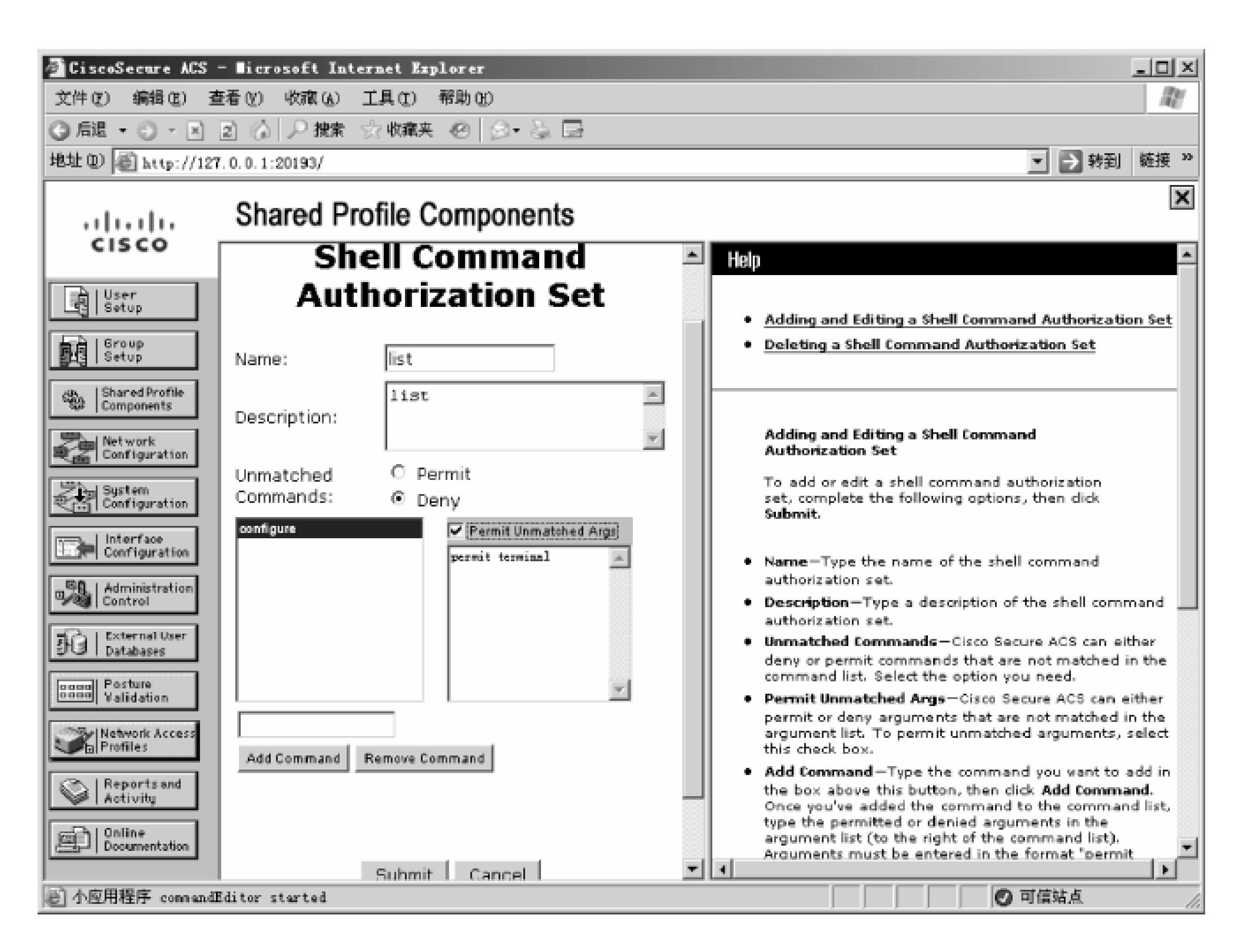


图 8-12 编辑命令集

（4）单击 Submit 按钮，保存设置，显示如图 8-13 所示的窗口。使用相同的方法可以创建多个自定义授权命令集。

4. 创建用户组

为了便于统一管理使用 ACS 服务器进行身份验证的用户账户，可以事先创建用户组，然后将不同需求的用户账户指派到不同的分组中，需要为用户授权时，直接对用户组进行操作即可。

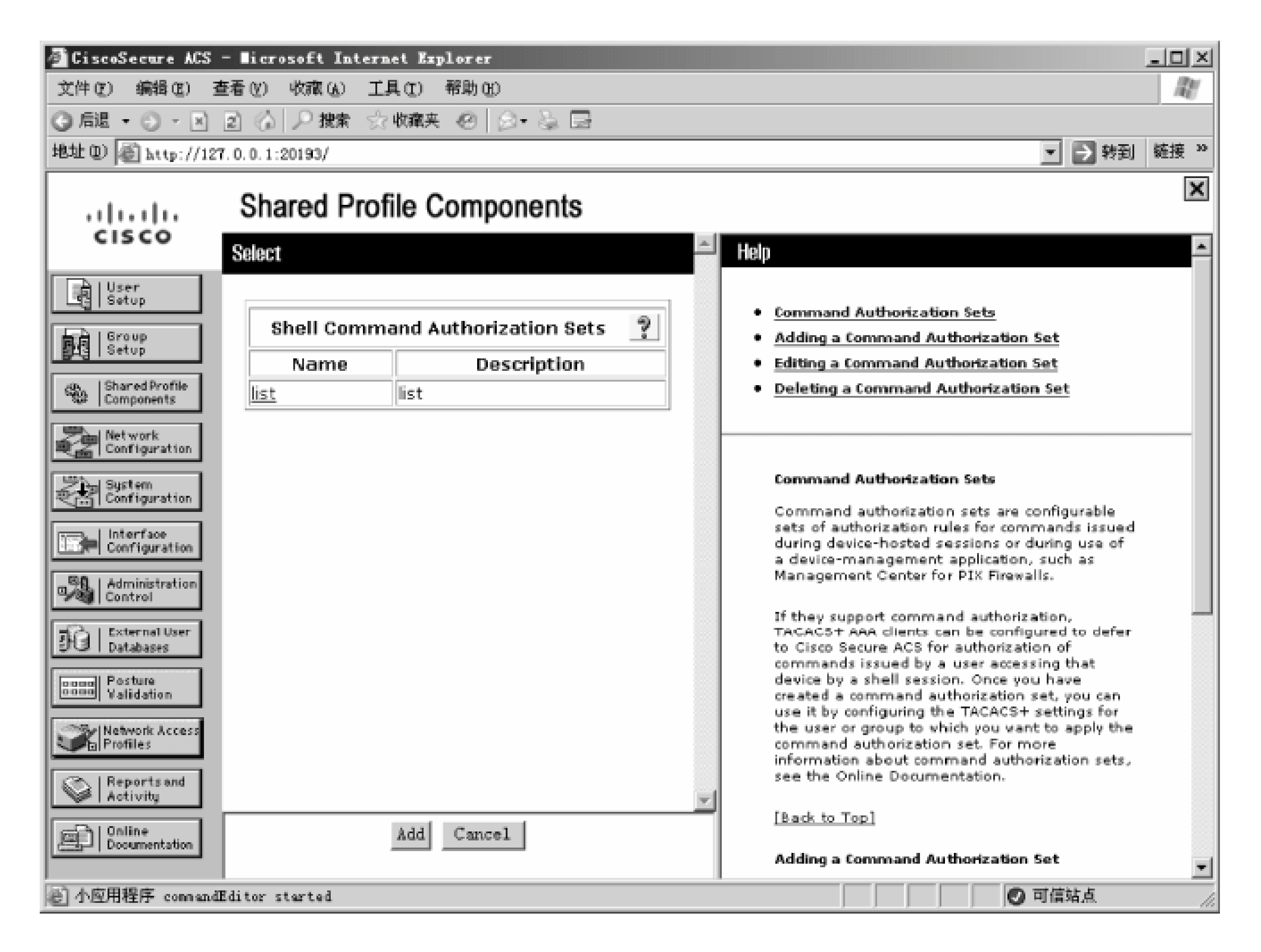


图 8-13　成功创建的命令集

(1) 在 ACS 管理窗口中，单击 Group Setup 按钮，显示如图 8-14 所示的窗口。默认情况下，ACS 服务器已经提供了 500 个用户组，默认组的名称是 Default Group，其他组名称是 Group 1～Group 499。

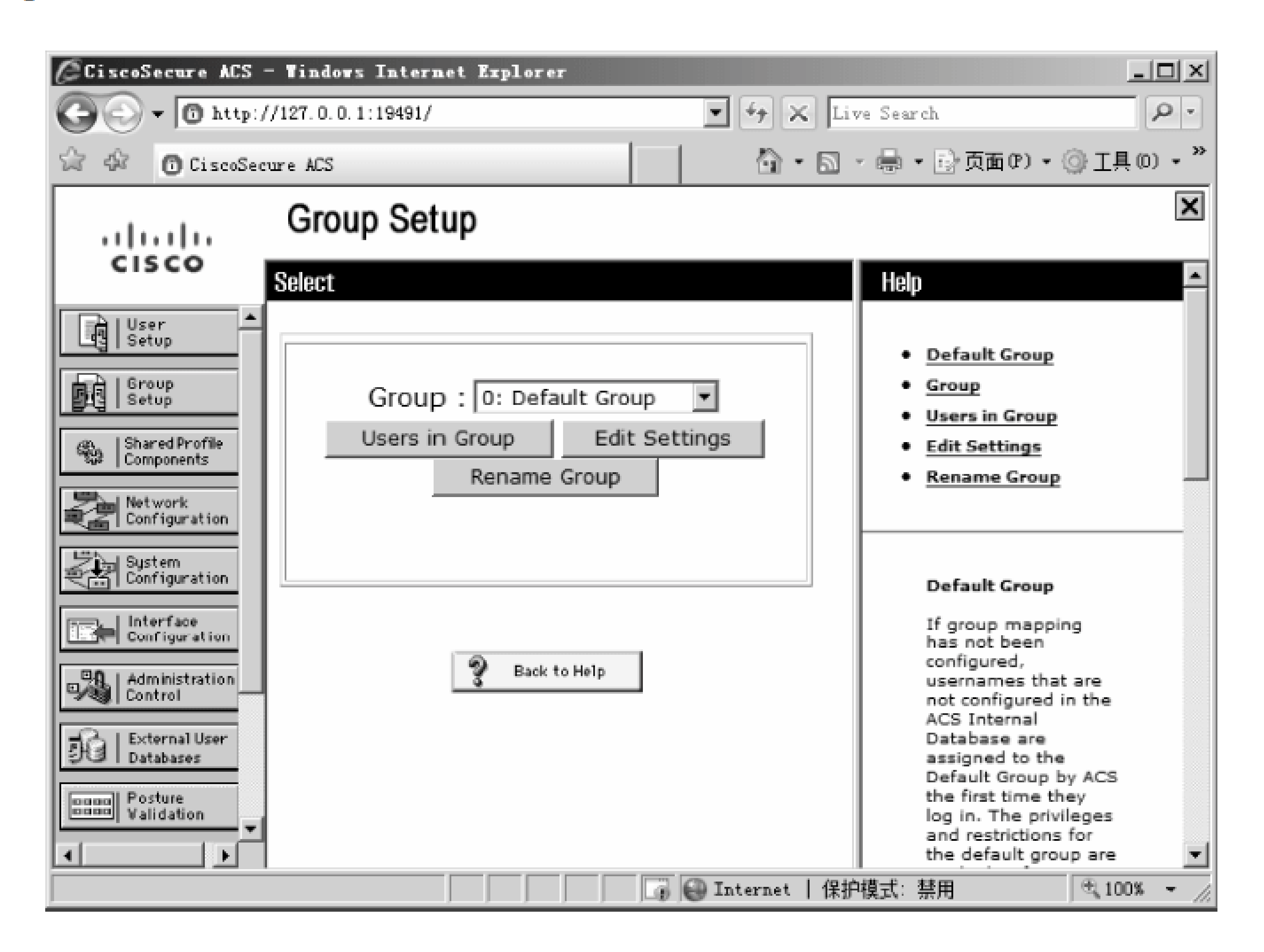


图 8-14　Group Setup 窗口

(2) 在 Group 下拉列表框中选择希望重命名的组，例如：Group 1，单击 Rename Group 按钮，显示如图 8-15 所示的 Renaming Group:Group 1 窗口。在 Group 文本框中输入新的组名称即可。

(3) 单击 Submit 按钮，保存设置并返回到 Group Setup 窗口。单击 Edit Settings 按钮，显示如图 8-16 所示的窗口，拖动滚动条至 Shell(exec)选项区域，选中 Shell(exec)复选框，即对组中的所有账户启用 Shell。

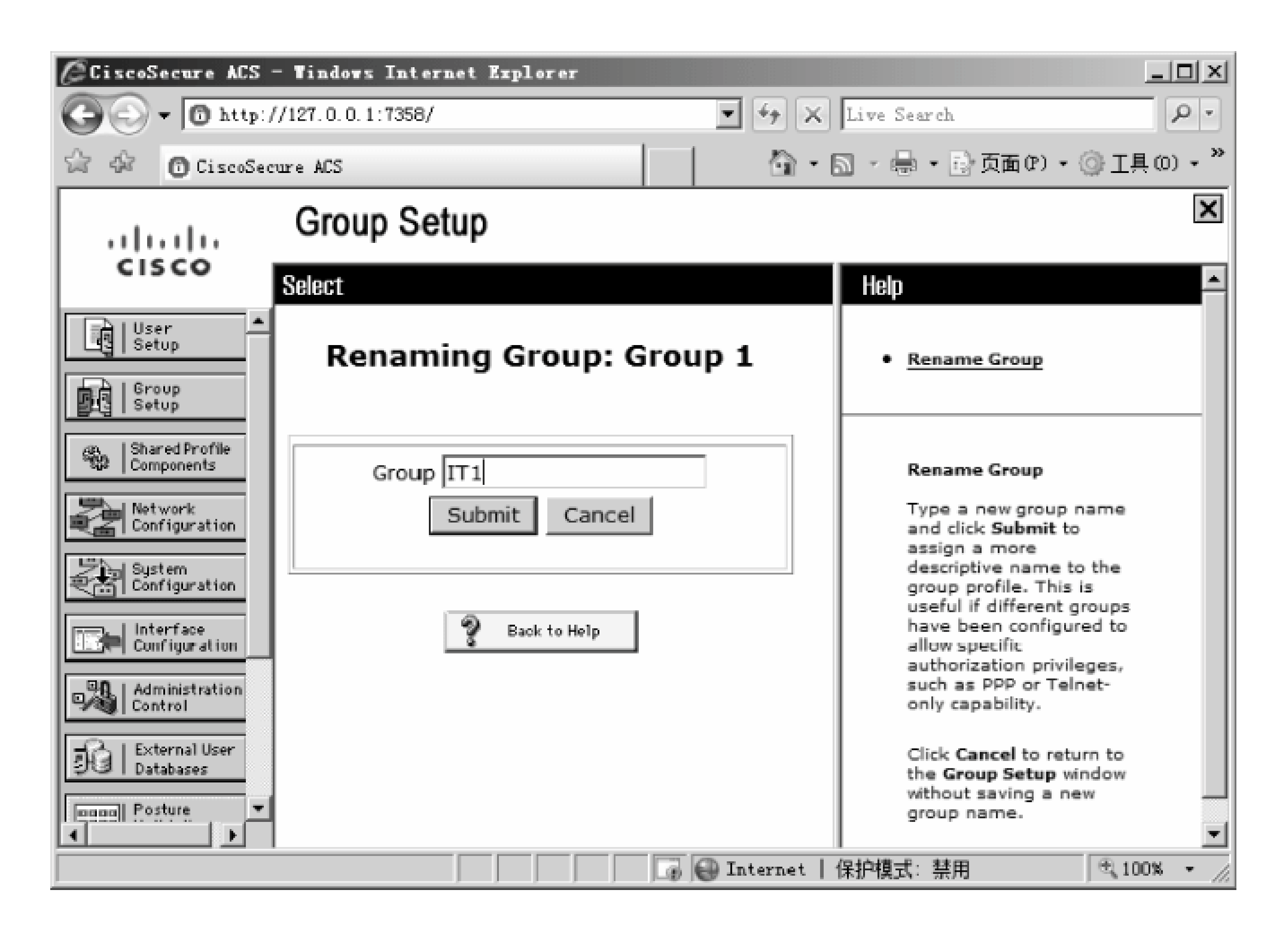


图 8-15 Renaming Group:Group 1 窗口

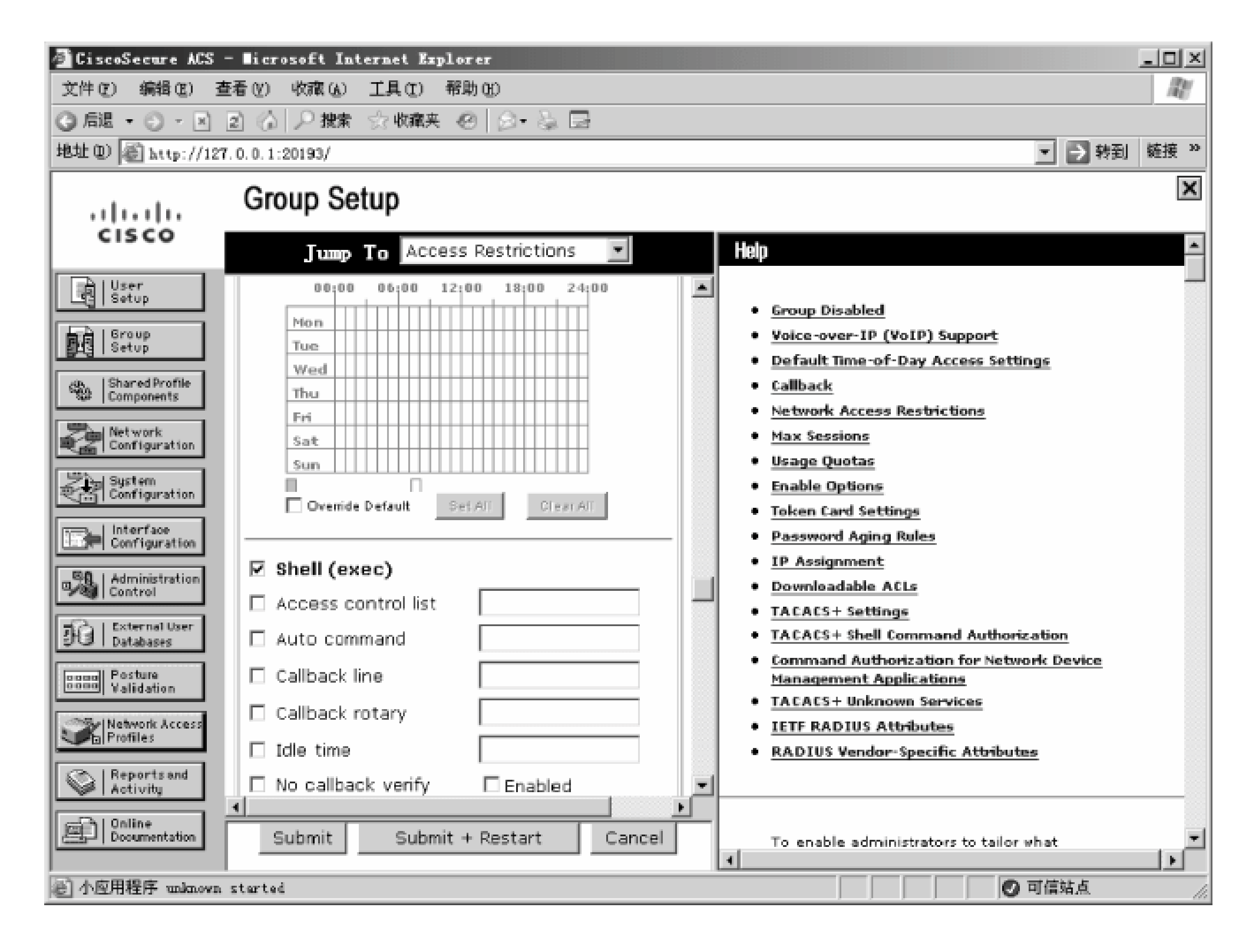


图 8-16 开启组的 Shell

(4) 单击 Submit 按钮,保存设置。

5. 创建用户账户

ACS 服务器的工作模式比较灵活,既可以基于当前域,也可以独立运行。如果基于现有域,则可以直接关联域中的指定用户组,使用户通过域用户账户登录网络设备,同时接受域控制器和 ACS 服务器的身份验证和记账服务。如果 ACS 服务器独立运行,则需要创建专用的用户账户。

(1) 在 ACS 服务器管理窗口中,单击 User Setup 按钮,显示如图 8-17 所示的 User Setup 窗口,在 User 文本框中输入用户名称,如 user1。应用过程中的用户管理也是在该窗口中进行的,单击 List all users 按钮,可以在右侧窗口中显示 ACS 服务器上的所有用户账户。

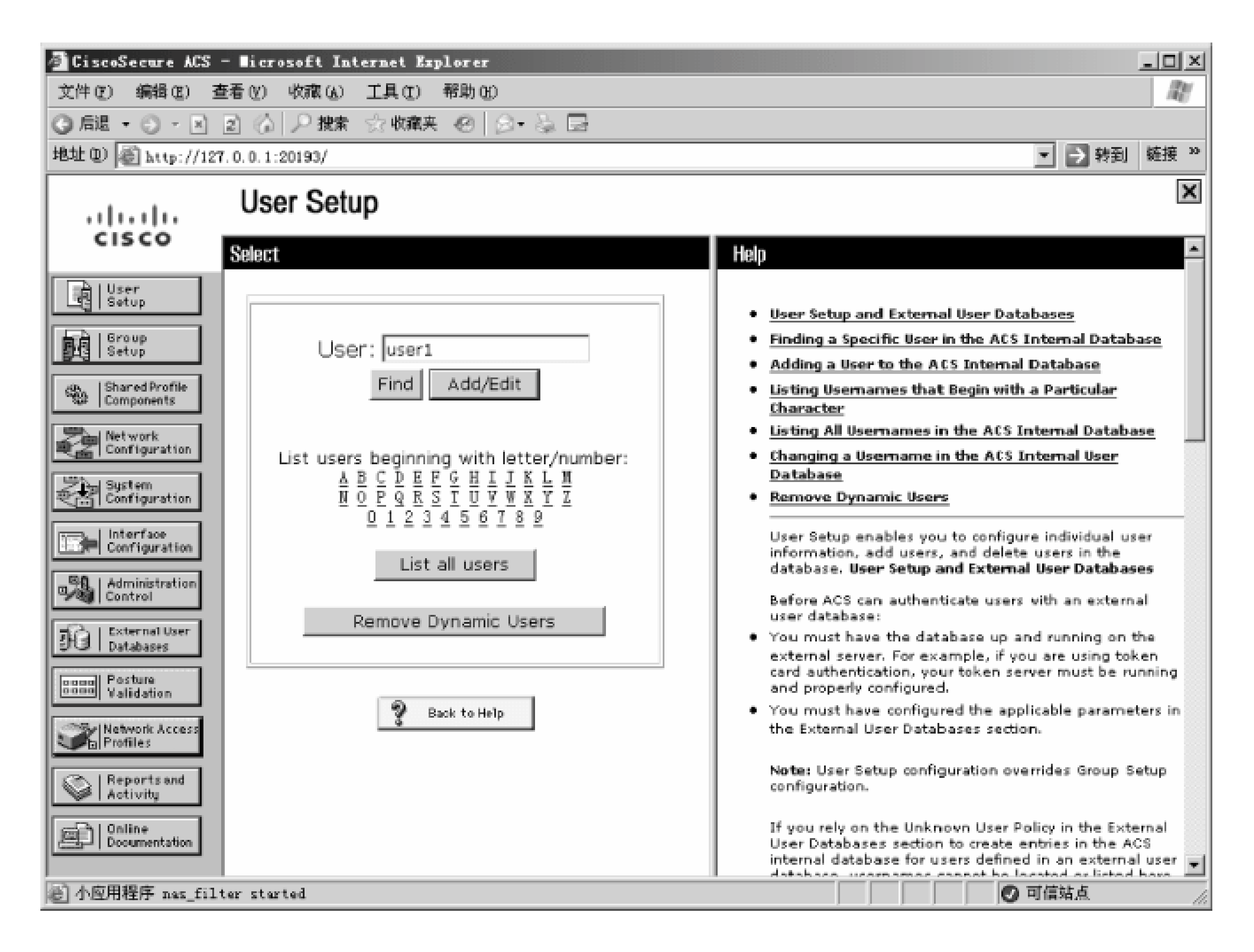


图 8-17 User Setup 窗口

(2) 单击 Add/Edit 按钮，显示如图 8-18 所示的窗口，在这里可以编辑用户账户相关信息。首先在 Supplementary User Info 选项区域设置用户账户的基本描述信息。

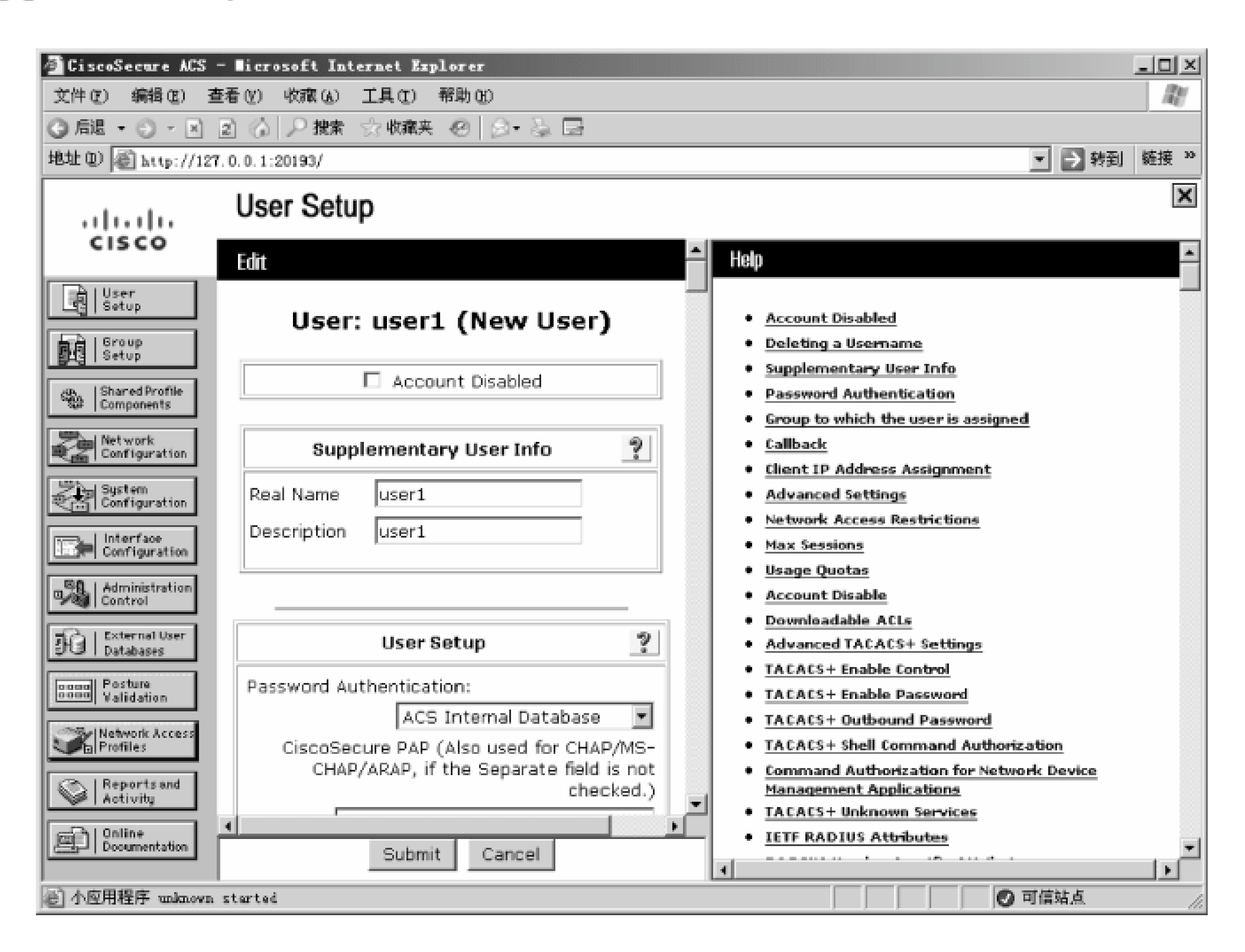


图 8-18 设置用户账户描述信息

(3) 为用户分配认证密码数据库并设置密码，如图 8-19 所示。向下拖动滚动条，在 User Setup 选项区域的 Password Authentication 下拉列表框中选择 ACS Internal Database 选项，即使用 ACS 内部数据库验证用户账户密码。如果 ACS 服务器是基于域的，则此处应选择 Windows Database 选项。在 Password 和 Confirm Password 文本框中输入用户账户密码。

(4) 将用户账户指派到组，如图 8-20 所示。为了便于统一管理，建议将用户账户指派到指定的组中，向下拖动滚动条，在 Group to which the user is assigned 下拉列表框中，选择希望将该用户账户指派到的组，例如 IT1。

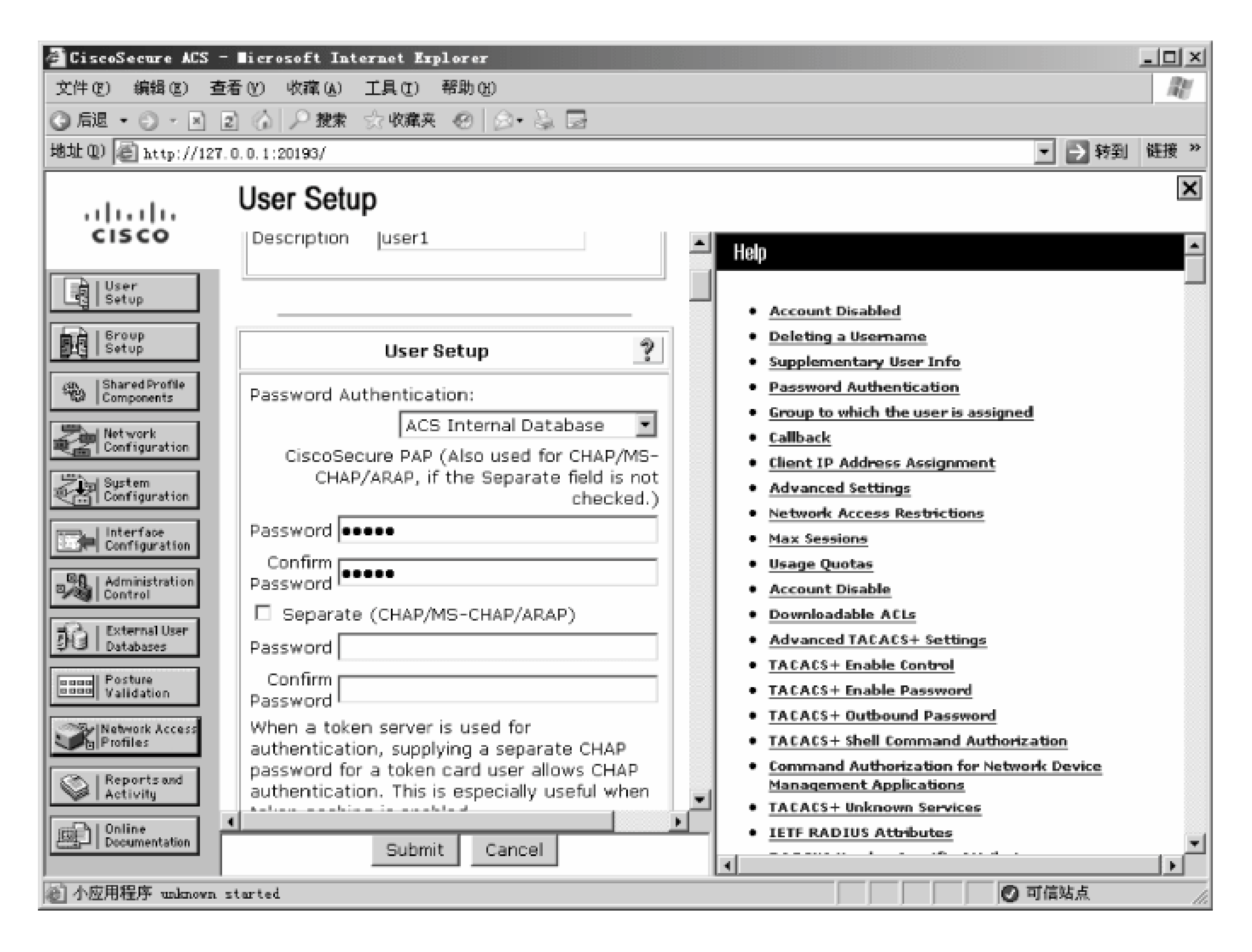


图 8-19　设置认证数据库和密码

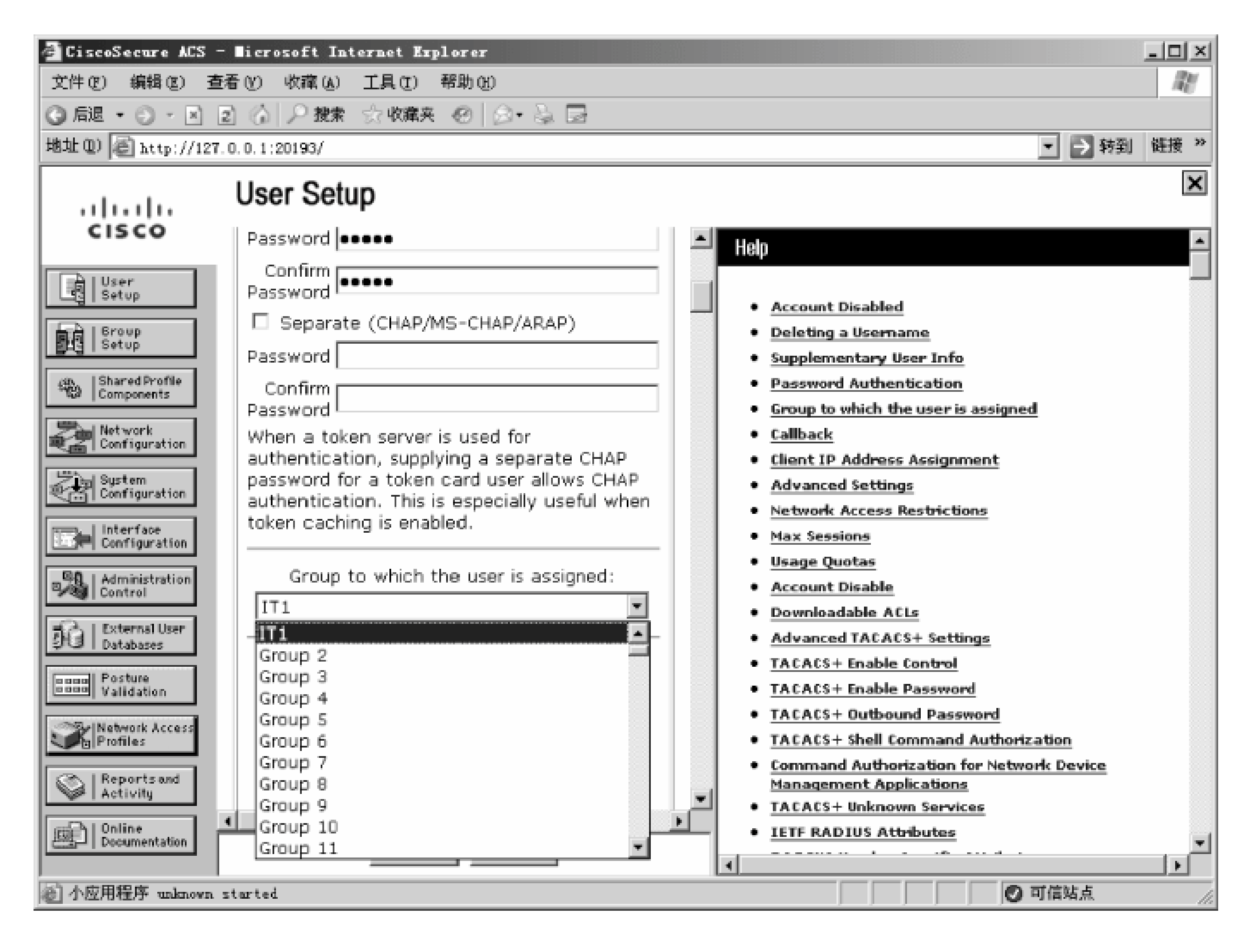


图 8-20　将用户账户指派到组

（5）为用户账户启用 Shell，如图 8-21 所示。为了使用 ACS 服务器对用户账户的操作命令行进行授权和记账，必须启用用户账户的 Shell。

如果用户所在组已经启用 Shell，则用户账户本身无须再启用，只需在 Shell Command Authorization Set 选项区域中选中 As Group 单选按钮即可，如图 8-22 所示。如果希望对所有操作命令进行授权和记账，则可以选中 Assign a Shell Command Authorization Set for any network device 单选按钮，并在其下拉列表框中选择实现编辑好的命令集即可，本例中选择的是前面创建的 list 命令集。

（6）单击 Submit 按钮，保存设置。

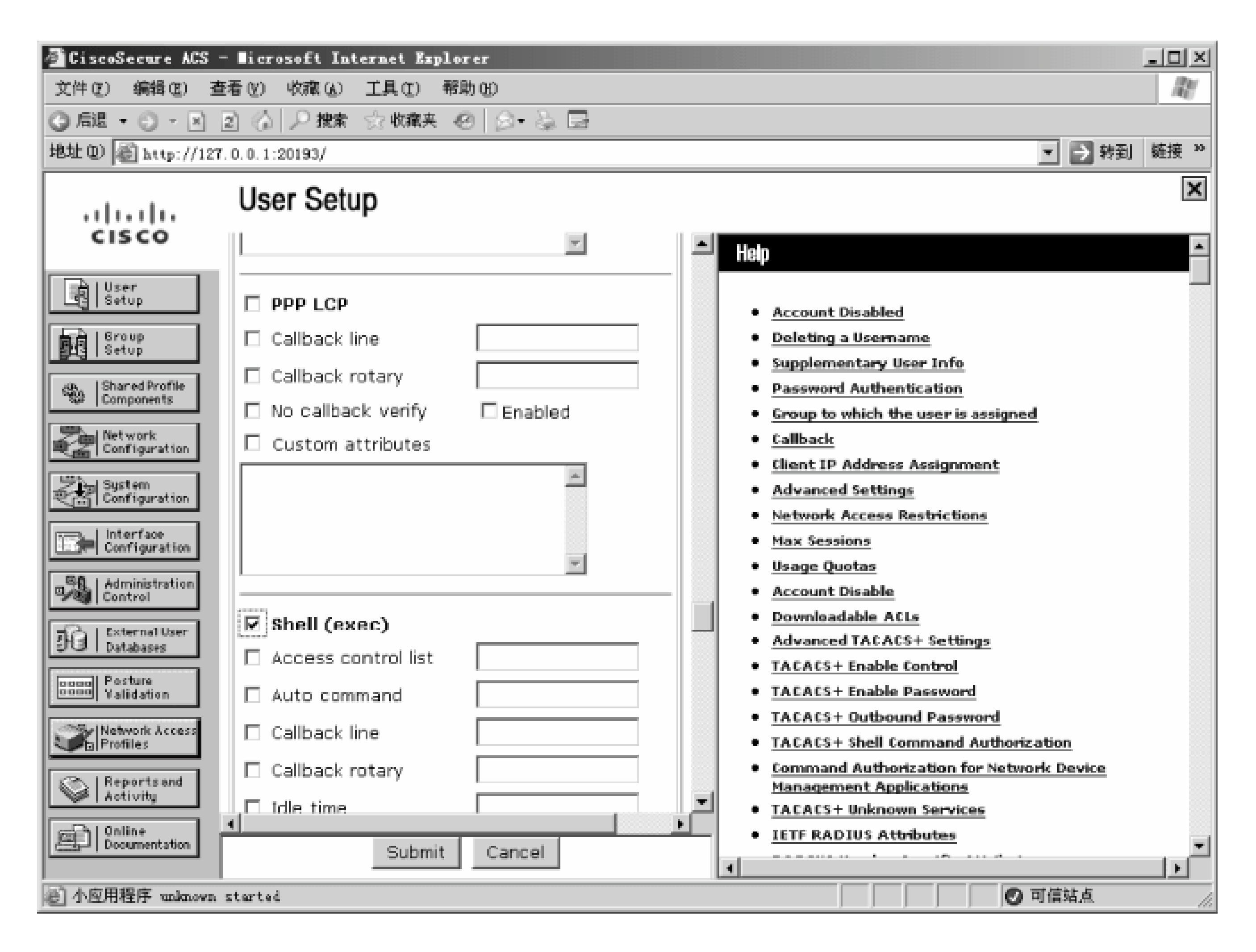


图 8-21　为用户账户启用 Shell

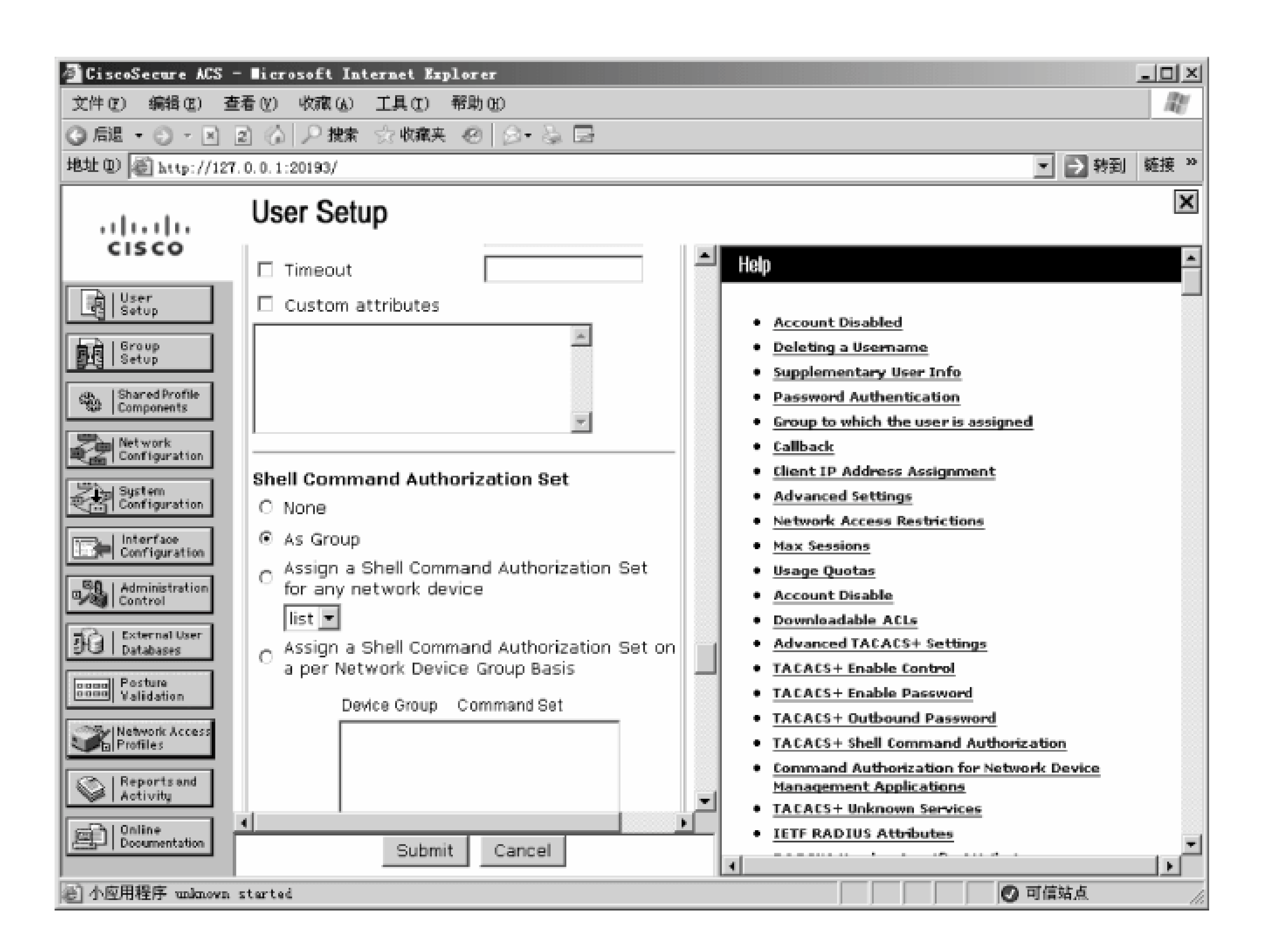


图 8-22　为用户应用组配置

提示：管理员可以根据需要自定义用户账户配置窗口中显示的选项。在 ACS 管理器窗口中，单击 Interface Configuration 按钮，显示如图 8-23 所示的 Interface Configuration 窗口，在 Advanced Options 列表中选中希望显示的选项即可，如果不明白选项对应的内容，建议全部选中。

6. 添加管理员账户

若要通过网络远程管理 ACS 服务器，则必须先创建用于远程管理的用户账户。在 ACS 管理窗口中，单击 Add Administrator 按钮，显示如图 8-24 所示的 Add Administrator 窗口。在 Administrator Details 选项区域设置用户名和密码。在 Administrator Privileges 选项区域，设置管理员的权限范围。

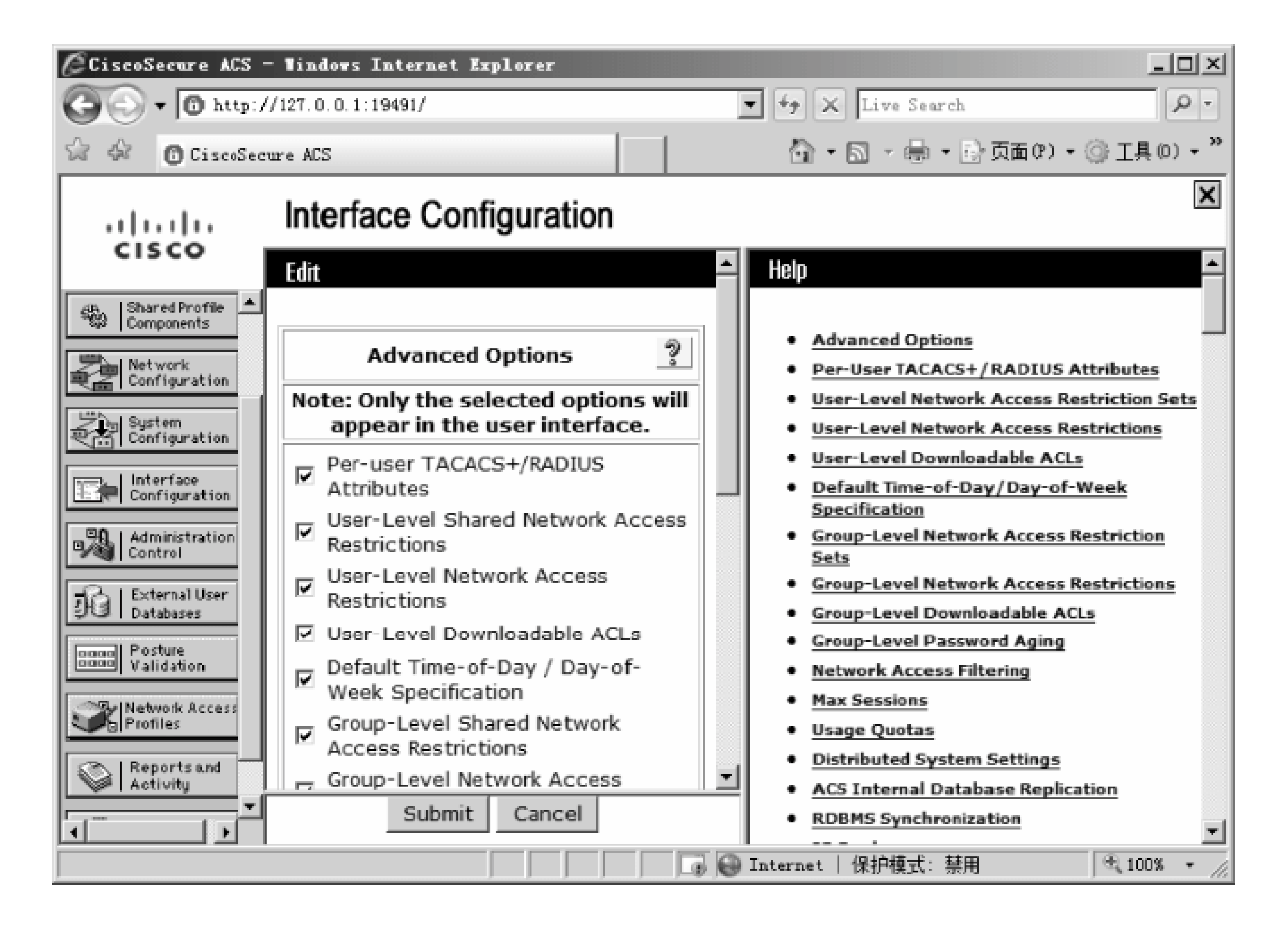


图 8-23 Interface Configuration 窗口

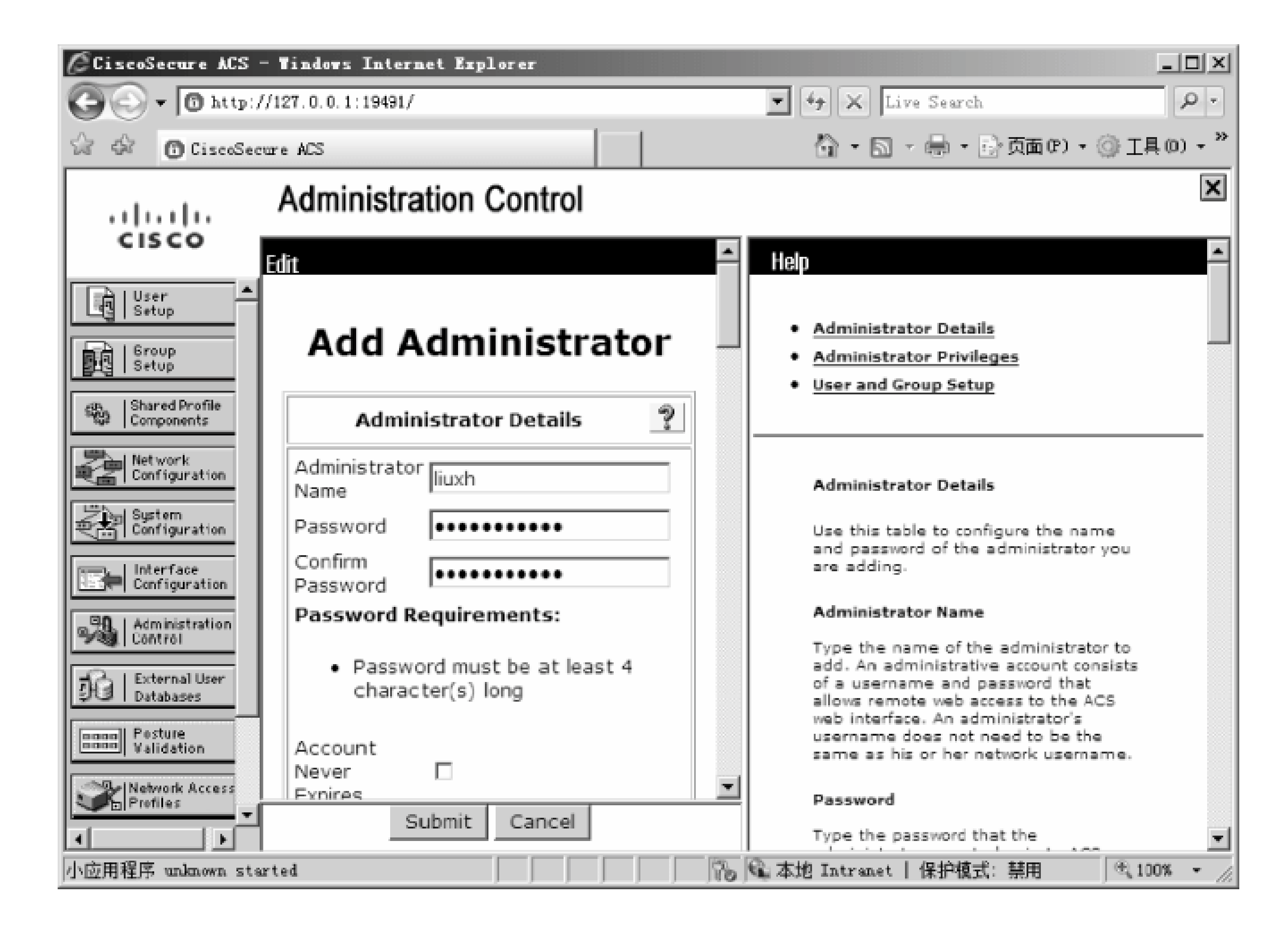


图 8-24 Add Administrator 窗口

8.2.4 管理 ACS 记账信息

ACS 服务器正常运行之后，即可自动对网络访问进行身份验证、授权和记账，同时生成相应的日志，管理员可以根据需要随时查看。默认情况下，ACS 服务器并未开启所有操作或授权的日志记录，管理员可以根据需要配置其自动生成的日志类型。

1. 配置日志功能

配置日志功能的操作步骤如下。

(1) 在 ACS 管理窗口中，单击 System Configuration 按钮，在显示的窗口中单击 Logging 链接，显示如图 8-25 所示的 ACS Reports 窗口。如果日志名称对应的配置状态为“×”，则表明禁用此日志功能，即不记录日志；否则将生成日志。

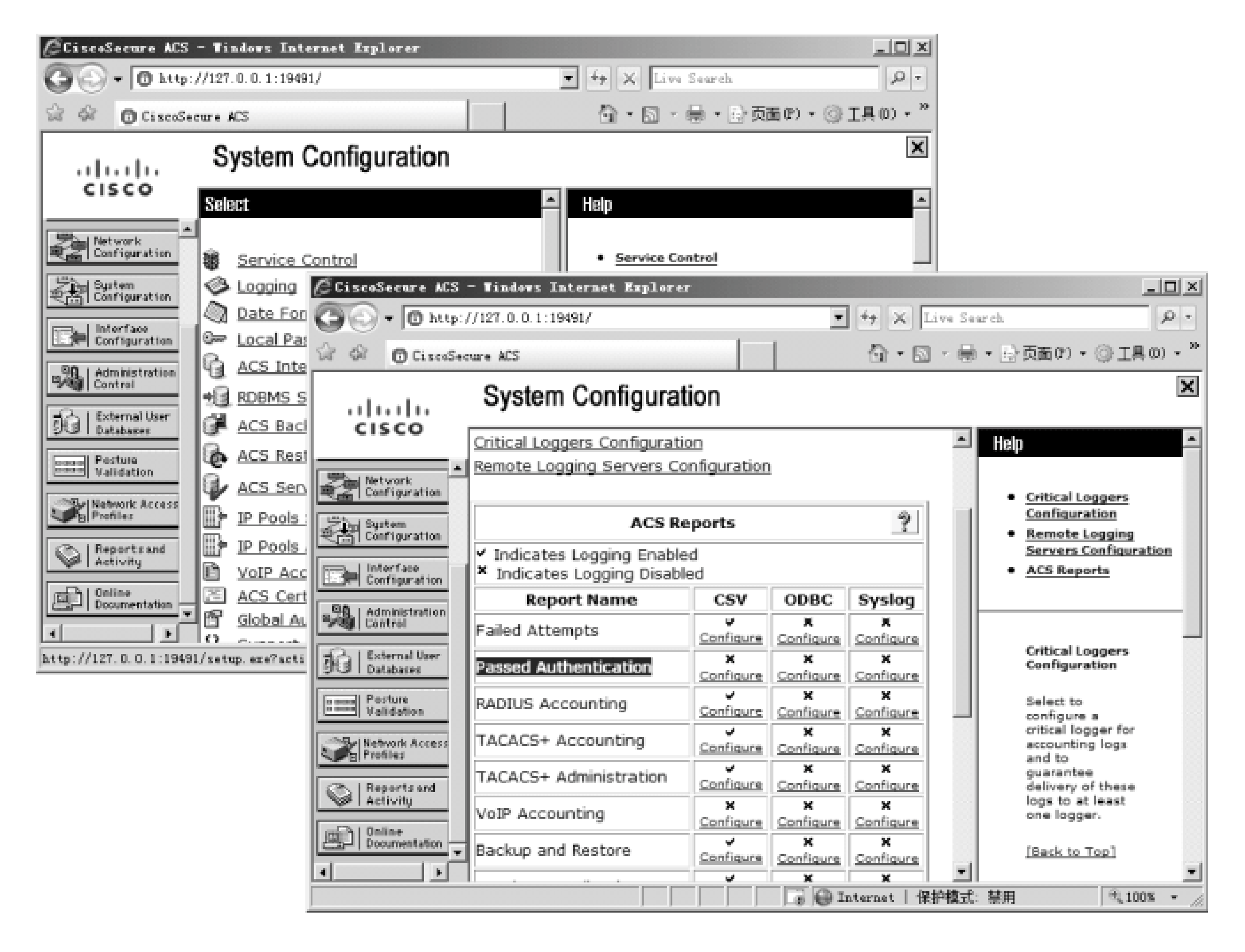


图 8-25　ACS Reports 窗口

(2) 以 Passed Authentication 为例，单击 CSV 列中的 Configuration 链接，显示如图 8-26 所示的 CSV Passed Authentications File Configuration 窗口，在 Enable Logging 选项区域内选中 Log to CSV Passed Authentications report 复选框，即启用该日志记录。在 Select Columns To Log 选项区域设置日志文件中显示的项目名称，在左侧列表中选中希望添加的项目，单击→按钮将其添加到右侧列表中。除此之外，还可以设置日志的保存路径、大小等。

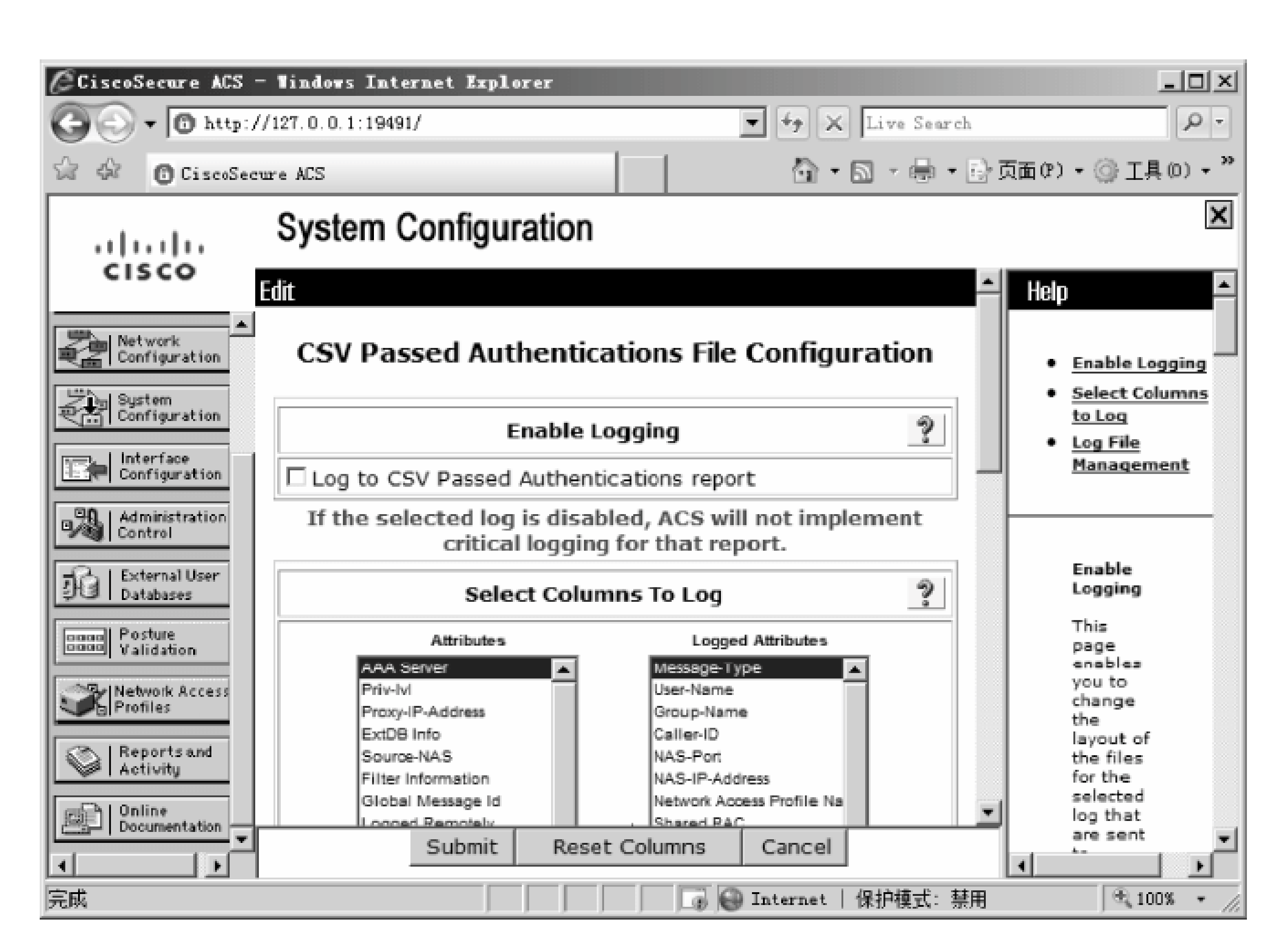


图 8-26　CSV Passed Authentications File Configuration 窗口

(3) 单击 Submit 按钮，保存设置。

2. 查看日志

(1) 在 ACS 管理窗口中，单击 Reports and Activity 按钮，显示如图 8-27 所示的 Reports 窗口。根据 ACS 服务器配置的身份验证项目的不同，生成的记账信息也会有所不同。例如，

单击 TACACS+Accounting 链接,在右侧列表中将显示所有的 TACACS+Accounting 记账信息。

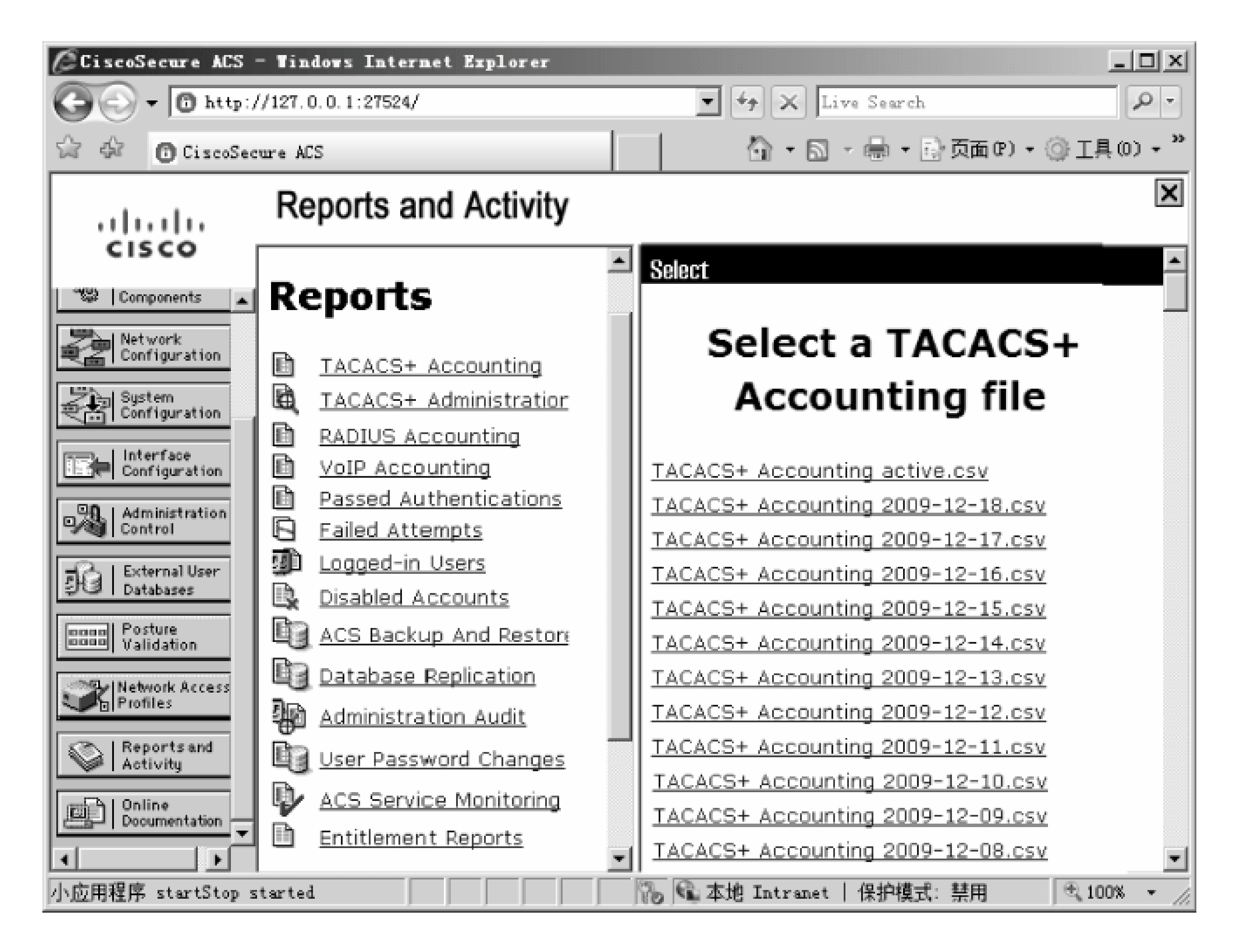


图 8-27 Reports 窗口

(2) 在右侧列表中按文件名中的日期检索希望查看的记账信息,单击文件名链接显示如图 8-28 所示的窗口,即可查看当前所有的登录记录。

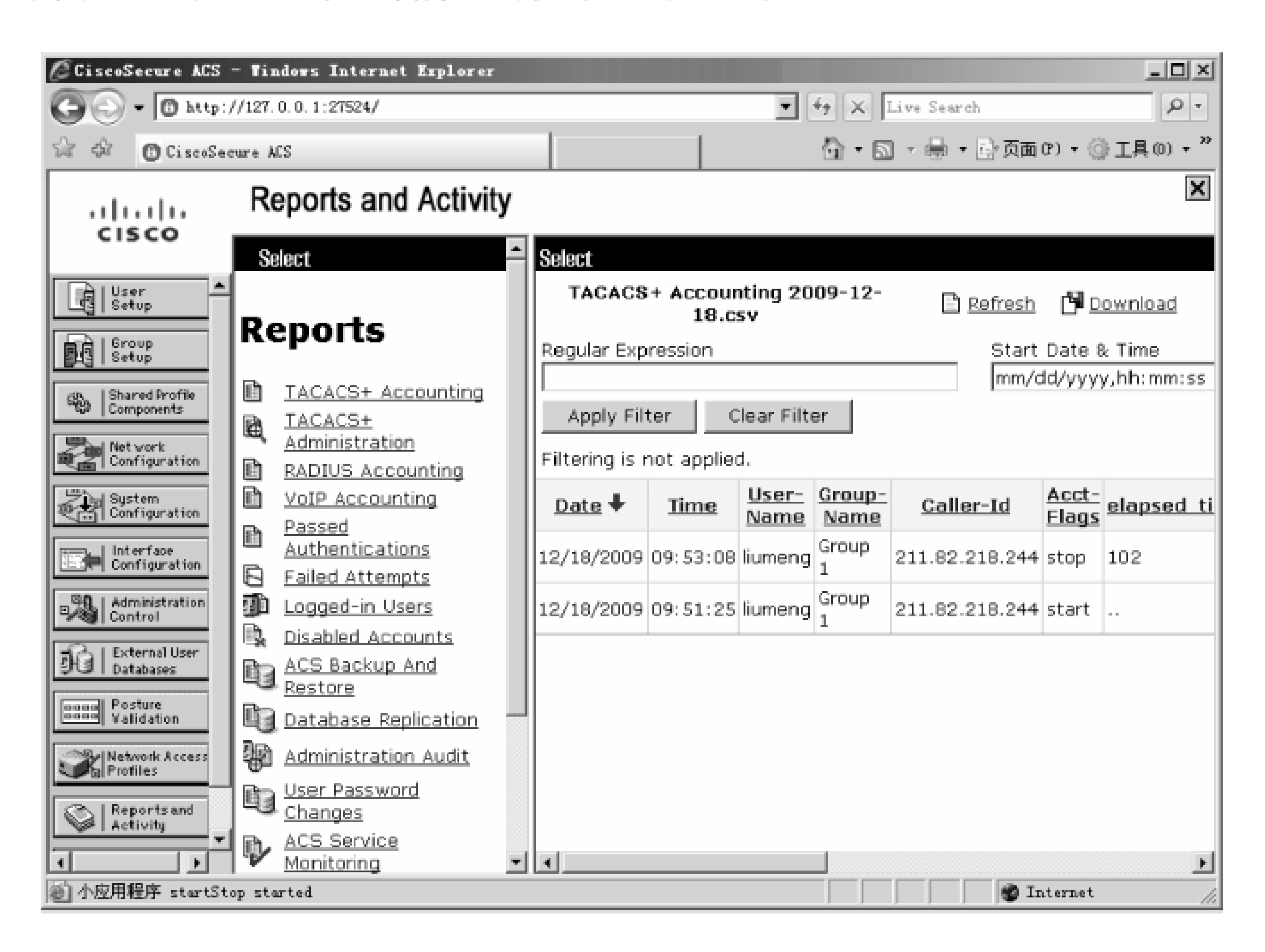


图 8-28 查看详细记账信息

8.3 基于 ACS 的基本认证

完成 ACS 服务器基本配置之后,即可开始为客户端提供身份验证和记账,将交换机配置为 ACS 客户端,在 ACS 服务器上对用户账户或组进行授权。当用户远程登录交换机进行管理时,将只能运行授权的命令并自动记账,非授权命令将无法运行。下面以使用 ACS

服务器对 15 级用户的操作命令作授权为例进行介绍。

8.3.1 配置交换机

在配置为 ACS 客户端的交换机上执行如下操作,即可配置为使用 ACS 服务器认证和记账,为客户端的操作进行授权。

(1) 进入全局配置模式。

```
HJ-3750# configure terminal
```

(2) 启用交换机的 AAA。

```
HJ-3750(config)# aaa new-model
```

(3) 指定用户账户登录授权。授权方式默认为使用 ACS 服务器的 TACACS+身份验证方式,如果失败则使用本地数据库进行身份验证。

```
HJ-3750(config)# aaa authentication login default group tacacs+local
```

(4) 指定命令行模式进行授权,采用的授权方式同上。

```
HJ-3750(config)# aaa authorization exec default group tacacs+local
```

(5) 指定对 15 级用户的命令行进行授权,采用的授权方式同上。

```
HJ-3750(config)# aaa authorization commands 15 default group tacacs+local
```

(6) 指定授权服务器的地址,即 ACS 服务器的 IP 地址。

```
HJ-3750(config)# tacacs-server host 192.168.100.3
```

(7) 指定客户端与 ACS 服务器通信时使用的共享密钥。

```
HJ-3750(config)# tacacs-server key cisco
```

(8) 返回特权模式。

```
HJ-3750(config-if)# end
```

(9) 保存配置。

```
HJ-3750# copy running-config startup-config
```

8.3.2 配置 ACS 服务器

ACS 默认对 show running-config、configure terminal 命令不作授权,下面通过自定义命令集对 user2 用户作 configure terminal 的命令授权。

(1) 创建自定义命令集并应用到 user2 用户账户,如图 8-29 所示。在 user2 的用户账户配置窗口中,选中 Assign a Shell Command Authorization Set for any network device 单选按钮,并在其下拉列表框中选择创建好的 list 命令集。命令集中命令的编辑方式可参考前面相关内容,此处不再赘述。

(2) 单击 Submit 按钮,保存配置。

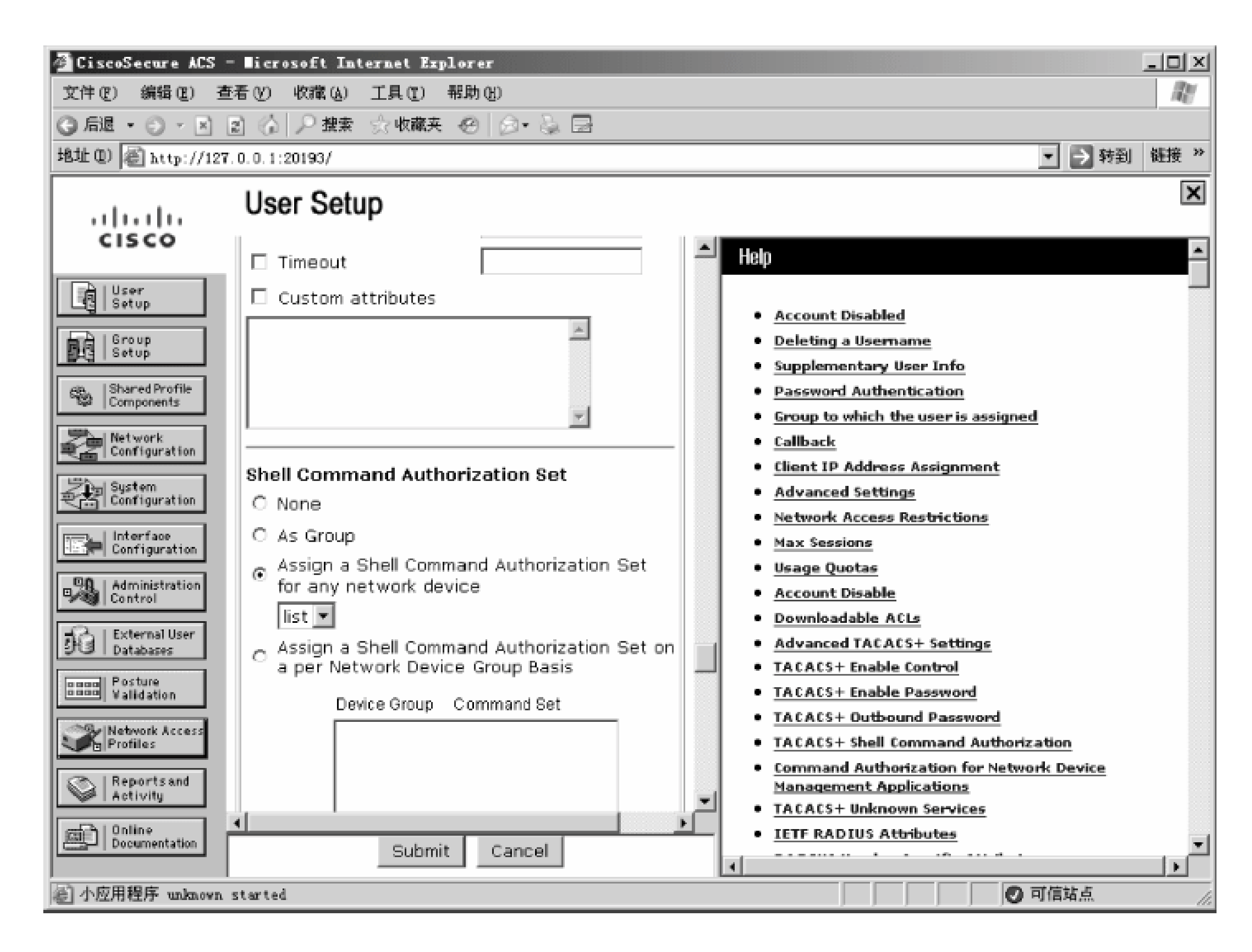


图 8-29 创建自定义命令集并应用到 user2 用户账户

8.3.3 用户登录测试

下面分别使用 user1 和 user2 用户账户远程登录交换机，测试授权结果。前面所作配置中授予 user2 运行 configure terminal 的权限，而 user1 未作任何授权。

（1）以 telnet 方式登录 IP 地址为 172.16.100.2 的交换机，由于启用了用户登录授权，所以会提示输入用户名和密码，如图 8-30 所示。默认情况下，以 telnet 方式登录是不需要用户名和密码的。

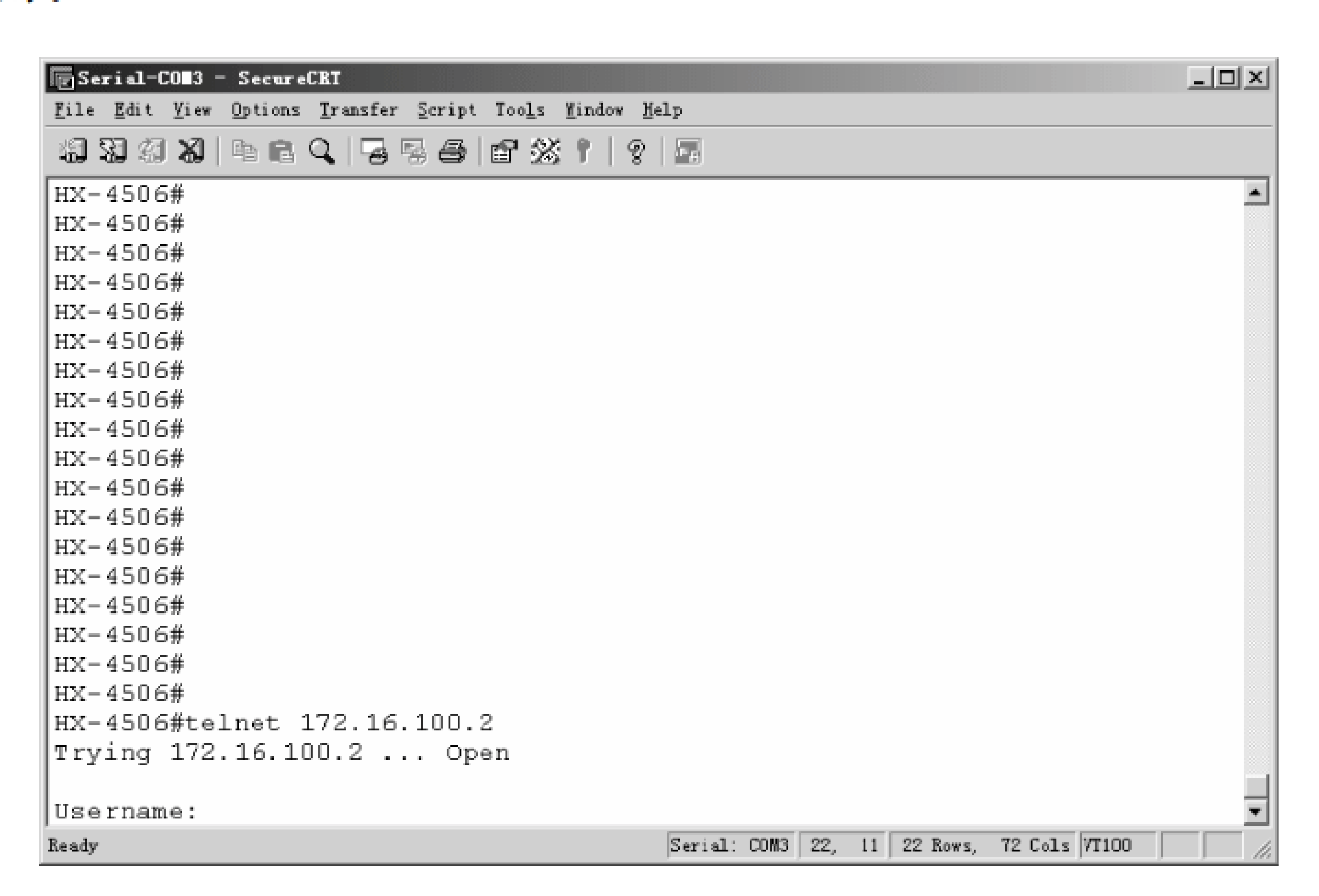


图 8-30 用户登录授权已启用

（2）以 user1 账户登录，输入 enable 命令进入全局配置模式，输入 show running-config 命令并运行，提示 Command authorization failed，即命令行认证失败，当前用户未被授权运行该命令。继续输入 configure terminal 命令并运行，结果相同，如图 8-31 所示。

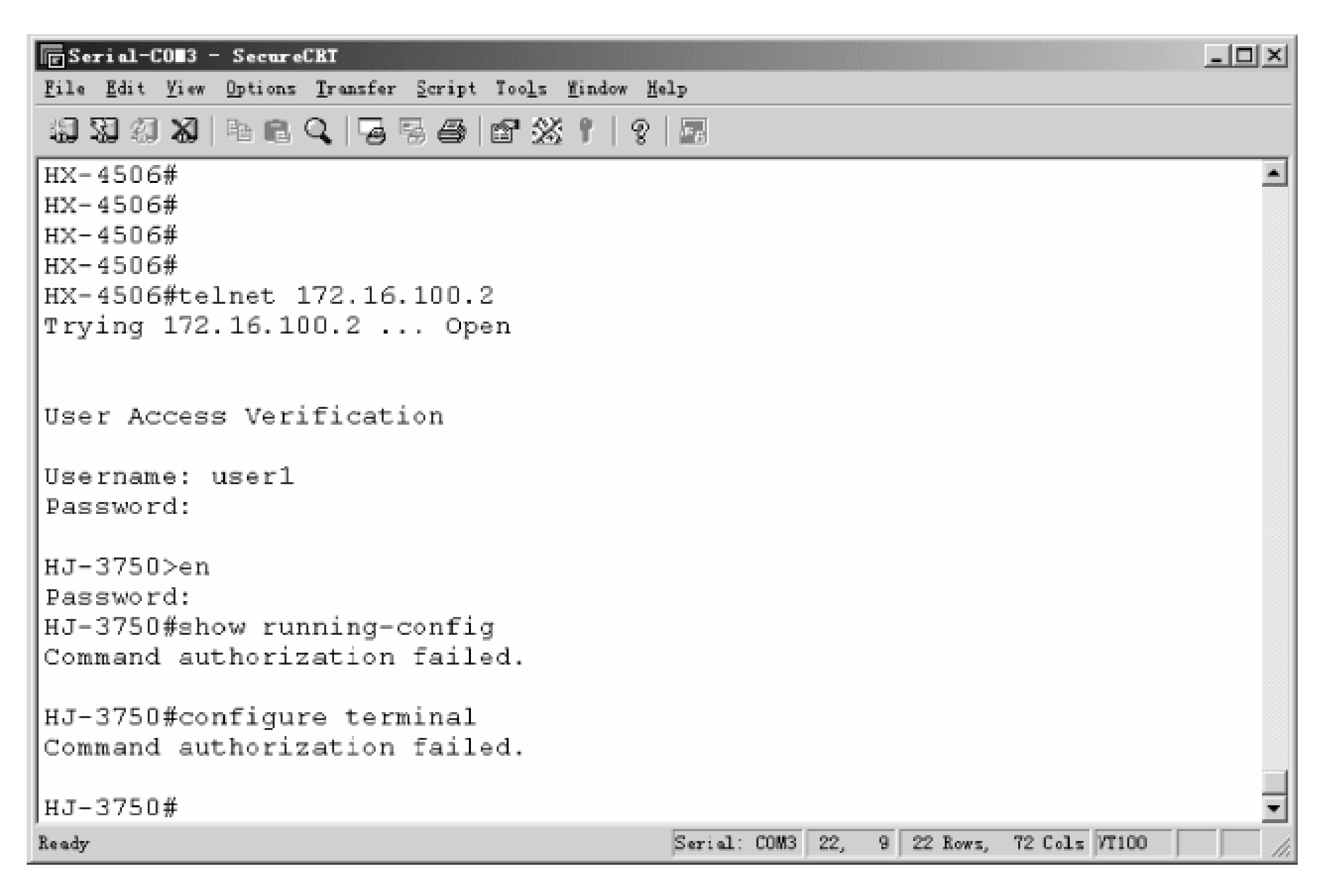


图 8-31　user1 账户未被授予操作任何命令的权限

（3）使用 user2 账户登录该交换机，同样进入全局配置模式，输入并运行 show running-config 命令时，提示命令行未被授权；输入并运行 configure terminal 命令时，命令成功运行，如图 8-32 所示，说明 user2 账户被授予运行 configure terminal 命令的权限，操作成功。

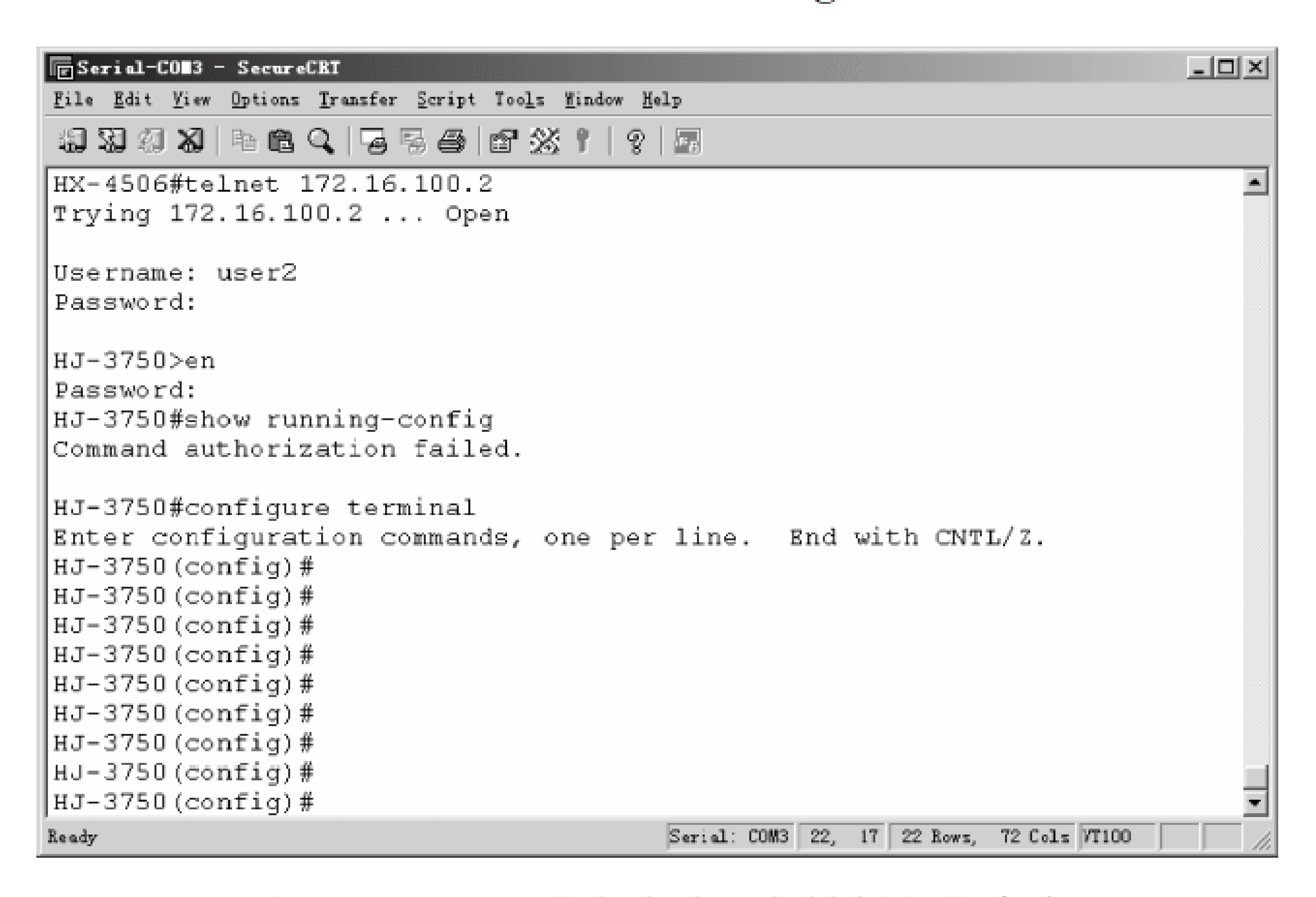


图 8-32　user2 账户成功运行被授权的命令

8.3.4　知识链接：ACS

1. CiscoSecure ACS

NAC 是 Cisco 公司推出的网络访问控制技术，可以使用网络基础设施迫使企图访问网络计算资源的所有设备遵守安全策略，进而防止病毒和蠕虫造成损失。而 CiscoSecure ACS 又是 Cisco NAC 架构的重要组件，是具有高可扩展性的高性能访问控制服务器，可作为集中的 RADIUS 和 TACACS+服务器运行。

CiscoSecure ACS 将验证、用户访问和管理员访问与策略控制结合在一个集中的身份识别网络解决方案中，因此提高了灵活性、移动性、安全性和用户生产率，从而进一步增强了访问安全性。它针对所有用户执行统一安全策略，不受用户网络访问方式的影响，减轻了与扩展用户和网络管理员访问权限相关的管理负担。通过对所有用户账户使用一个集中数据

库,CiscoSecure ACS 可集中控制所有的用户权限并将其分配到网络中的几百甚至几千个接入点。对于记账服务,CiscoSecure ACS 针对网络用户的行为提供具体的报告和监控功能,并记录整个网络上每次的访问连接和设备配置变化。CiscoSecure ACS 支持广泛的访问连接,包括有线和无线局域网、宽带、内容、存储、VoIP、防火墙和 VPN 等。

CiscoSecure ACS 是功能强大的访问控制服务器,为正在增加其 WAN 或 LAN 连接的机构提供了许多高性能和可扩展性特性。表 8-1 显示了 CiscoSecure ACS 的主要优势。

表 8-1　CiscoSecure ACS 的主要优势

优　　势	描　　述
易用性	基于 Web 的用户界面可简化并分发用户资料、组资料和 CiscoSecure ACS 的配置
可扩展性	CiscoSecure ACS 可通过支持冗余服务器、远程数据库以及数据库复制和备份服务来支持大型网络环境
可扩容性	轻型目录访问协议(LDAP)验证转发功能支持对著名目录供应商保存在目录中的用户资料进行验证,包括 Sun、Novell 和 Microsoft 等
管理	Windows Active Directory 支持结合了 Windows 用户名和密码管理功能,并使用 Windows Performance Monitor 来查看实时统计数据
系统管理	为每个 CiscoSecure ACS 管理员分配不同的访问权限,以及对网络设备进行分组的能力,可以更轻松地控制网络访问并最大限度地提高灵活性,从而方便地对网络中的所有设备执行并更改安全策略
产品灵活性	Cisco IOS 软件内嵌了对于 AAA 的支持,因此,CiscoSecure ACS 几乎能在思科销售的任何网络接入服务器上使用(Cisco IOS 软件版本必须支持 RADIUS 或 TACACS+)
集成	与 Cisco IOS 路由器和 VPN 解决方案紧密集成,提供了多机箱多链路点到点协议(PPP)和 Cisco IOS 软件命令授权等特性
第三方支持	CiscoSecure ACS 为提供满足 RFC 要求的 RADIUS 接口(如 RSA、PassGo、安全计算、ActiveCard、Vasco 或 CryptoCard)的所有 OTP 供应商提供令牌服务器支持
控制	CiscoSecure ACS 为一天中的时间点、网络使用、登录的会话数量和一周中每天的访问限制提供动态配额

2. ACS 应用环境

基于 Windows 系统服务器的 CiscoSecure ACS 服务器适用于如下需求环境。

(1) 集中控制用户通过有线或者无线连接登录网络。

(2) 设置每个网络用户的权限。

(3) 记录记账信息,包括安全审查或者用户记账。

(4) 设置每个配置管理员的访问权限和控制指令。

(5) 用于 Aironet 密钥重设置的虚拟 VSA。

(6) 安全的服务器权限和加密。

(7) 通过动态端口分配简化防火墙接入和控制。

(8) 统一的用户 AAA 服务。

8.4　基于 ACS 的 802.1x 认证

IEEE 802.1x 身份验证用于对有线以太网和无线 IEEE 802.11 网络进行经过身份验证的网络访问。IEEE 802.1x 通过提供对集中式用户标识、身份验证、动态密钥管理和记账的

支持来提高安全性和部署,执行基于端口的网络访问控制。基于端口的网络访问控制使用局域网基础设施的物理特征来验证连接到 LAN 端口的设备,并防止访问身份验证进程已经失败的那个端口。

8.4.1 交换机的 802.1x 认证

若欲实现 IEEE 802.1x 认证,必须在 Cisco 交换机上作必要的配置,启用 802.1x 身份验证功能。目前,企业网络中已经部署了 ACS 服务器,因此可以使用 ACS 服务器为交换机进行身份验证。

1. 交换机的配置

执行如下操作,即可在交换机上启用 IEEE 802.1x 认证,实现用户登录认证。

(1) 进入全局配置模式。

```
JR-2960-1# configure terminal
```

(2) 启用 AAA。

```
JR-2960-1(config)# aaa new-model
```

(3) 创建 IEEE 802.1x AAA 认证方式列表。如果在认证命令中没有指定列表名称,将创建并使用一个默认列表。默认情形下,将使用认证方式后的默认关键字。默认认证方式自动应用于所有接口。输入下列至少一个关键字,group radius 使用列表中所有的 RADIUS 服务器认证;none 不认证,客户端自动通过交换机认证,而无须使用客户端支持信息。

```
JR-2960-1(config)# aaa authentication dot1x default group radius local
```

(4) 指定提供 AAA 服务的服务器,即 ACS 服务器。

```
JR-2960-1(config)# radius-server host 192.168.100.3
```

(5) 指定与 ACS 服务器通信时使用的共享密钥,必须与 ACS 服务器端的设置完全相同,这里使用 cisco。

```
JR-2960-1(config)# radius-server key cisco
```

(6) 在交换机上启用 IEEE 802.1x 认证。

```
JR-2960-1(config)# dot1x system-auth-control
```

(7) 指定欲启用 IEEE 802.1x 认证的端口。

```
JR-2960-1(config)# interface fastEthernet 0/6
```

(8) 在该端口启用 802.1x 认证。

```
JR-2960-1(config-if)# dot1x port-control auto
```

(9) 指定向用户计算机发送 802.1x 身份验证信息的周期为 45 秒。

```
JR-2960-1(config-if)# dot1x timeout reauth-period 45
```

（10）返回特权模式。

```
JR-2960-1(config-if)# end
```

（11）查看配置是否正确。

```
JR-2960-1# show dot1x
```

（12）保存配置。

```
JR-2960-1# copy running-config startup-config
```

提示：若欲在多个端口启用 IEEE 802.1x 认证，应当重复指定端口和启用认证的操作，或者将相同配置的端口设置为一个端口组，然后配置该端口组。

2．ACS 服务器的配置

使用 ACS 服务器为交换机提供身份验证功能之前，必须将交换机配置为 ACS 客户端，并为用户账户或组授权。

（1）在 ACS 管理窗口中，单击 Network Configuration 按钮，可以管理现有 ACS 客户端或添加客户端。默认情况下，ACS 服务器没有任何客户端。在 Network Device Group 选项区域内单击 Add Entry 按钮，显示如图 8-33 所示的 New Network Device Group 窗口。在 Network Device Group Name 文本框中输入客户端组名，如 coolpen。

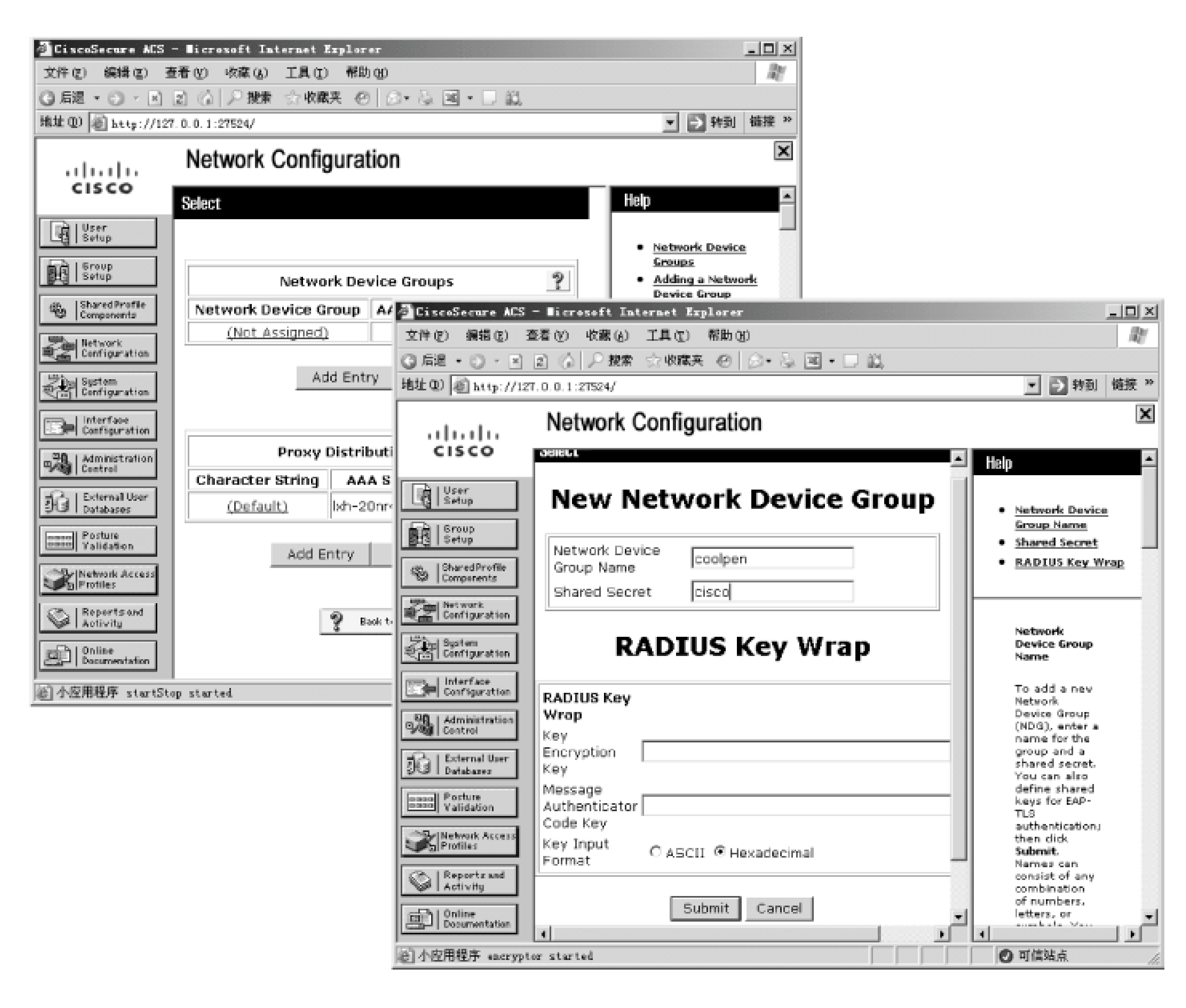


图 8-33 Net Network Device Group 窗口

（2）单击 Submit 按钮，保存设置并返回 Network Configuration 窗口，coolpen 就是成功创建的客户端组，如图 8-34 所示。

（3）单击 coolpen 链接，显示如图 8-35 所示的窗口，默认情况下该组中没有任何客户端。

（4）在 coolpen AAA Clients 选项区域内单击 Add Entry 按钮，显示如图 8-36 所示的

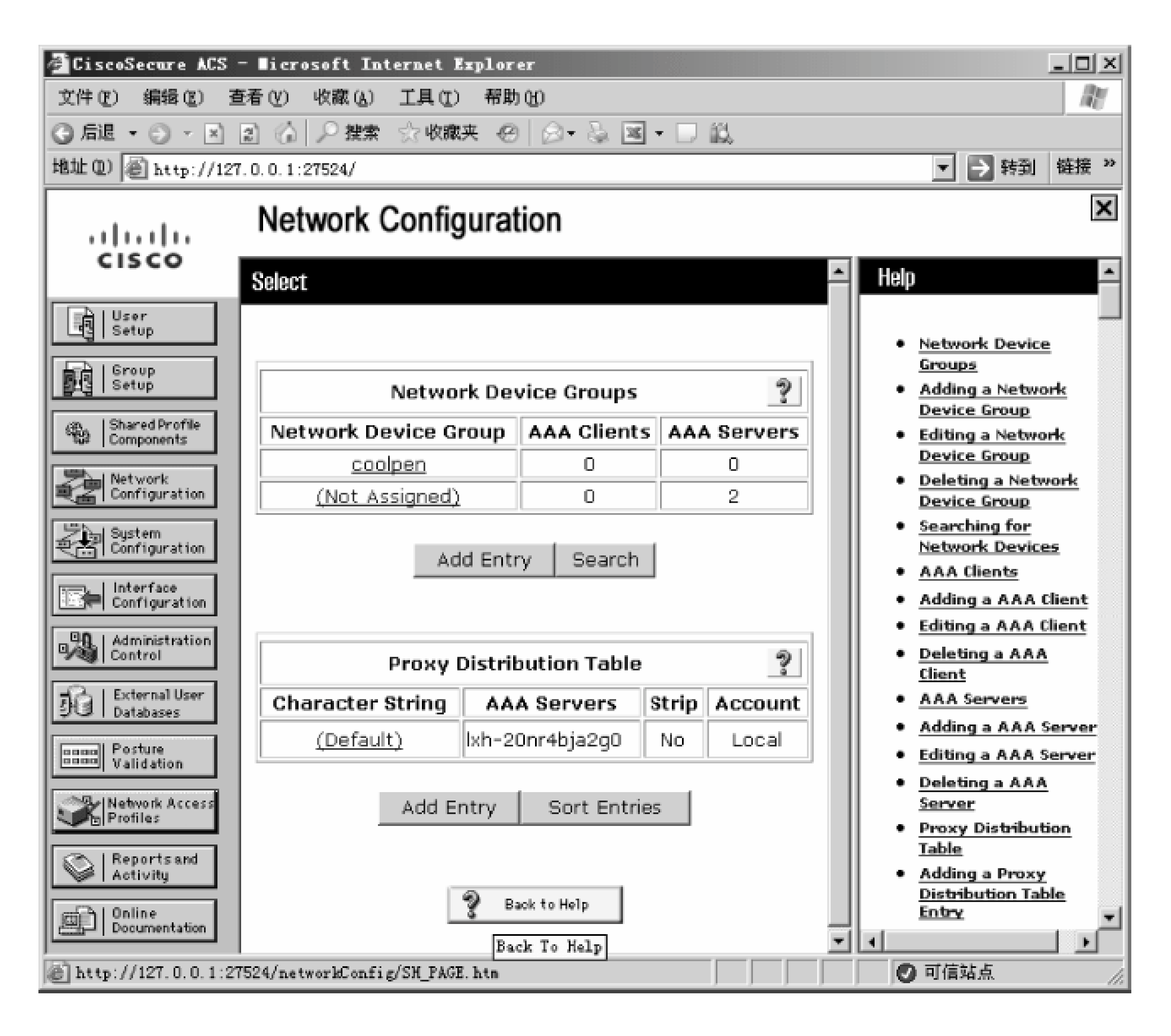


图 8-34　成功创建客户端组

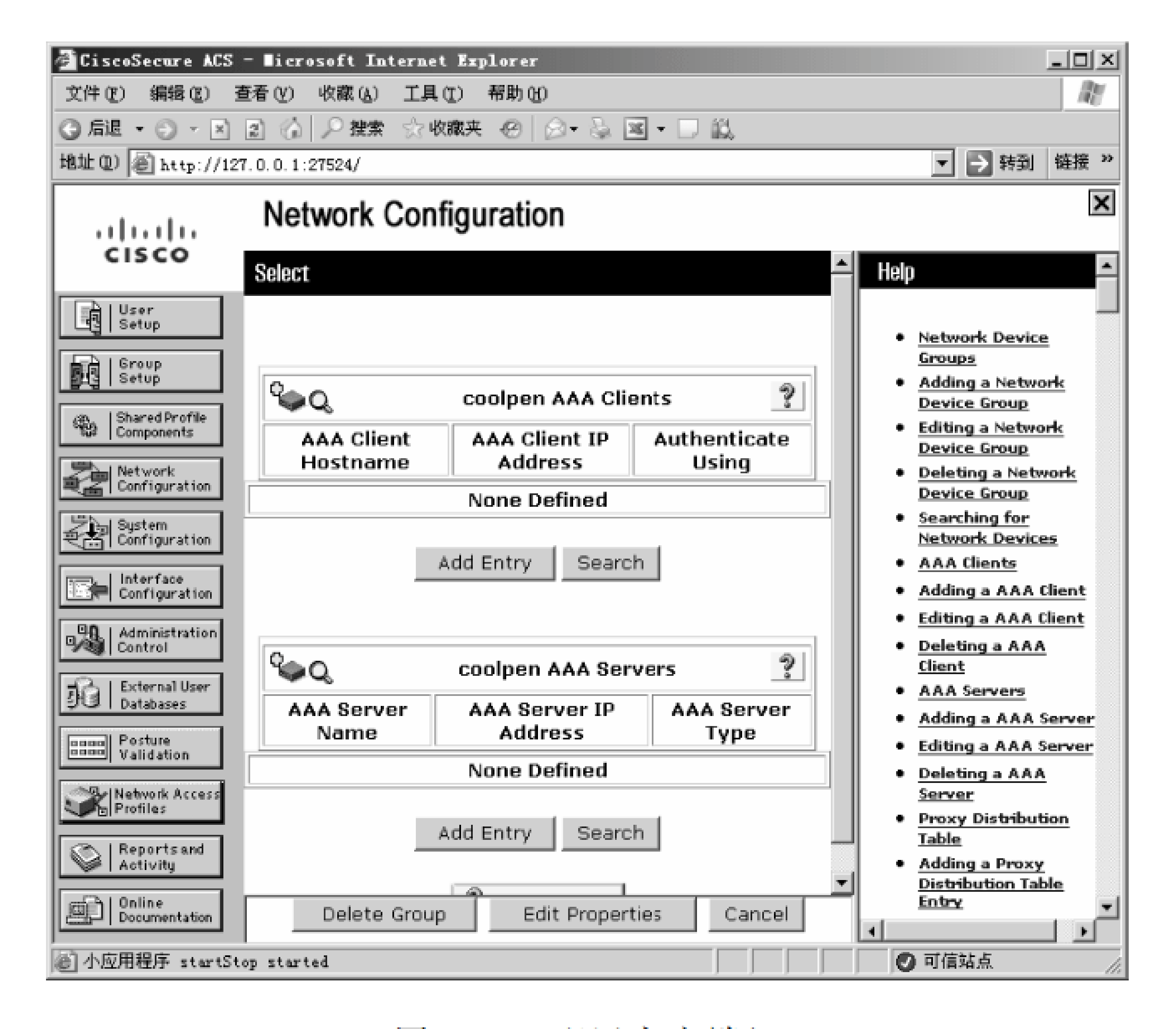


图 8-35　配置客户端组

Add AAA Client 窗口。在 AAA Client Hostname 文本框中，输入交换机的主机名；在 AAA Client IP Address 文本框中输入交换机的 IP 地址；在 Shared Secret 文本框中输入密钥(必须与交换机上使用的共享密钥相同)；在 Network Device Group 下拉列表框中选择添加到的客户端组，这里选择 coolpen，默认情况下是未指派的。

(5) 设置身份验证方式。在 Authenticate Using 下拉列表框中选择 RADIUS(IETF)选项，选中 Log Update/Watchdog Packets from this AAA Client 复选框，记录来自 AAA

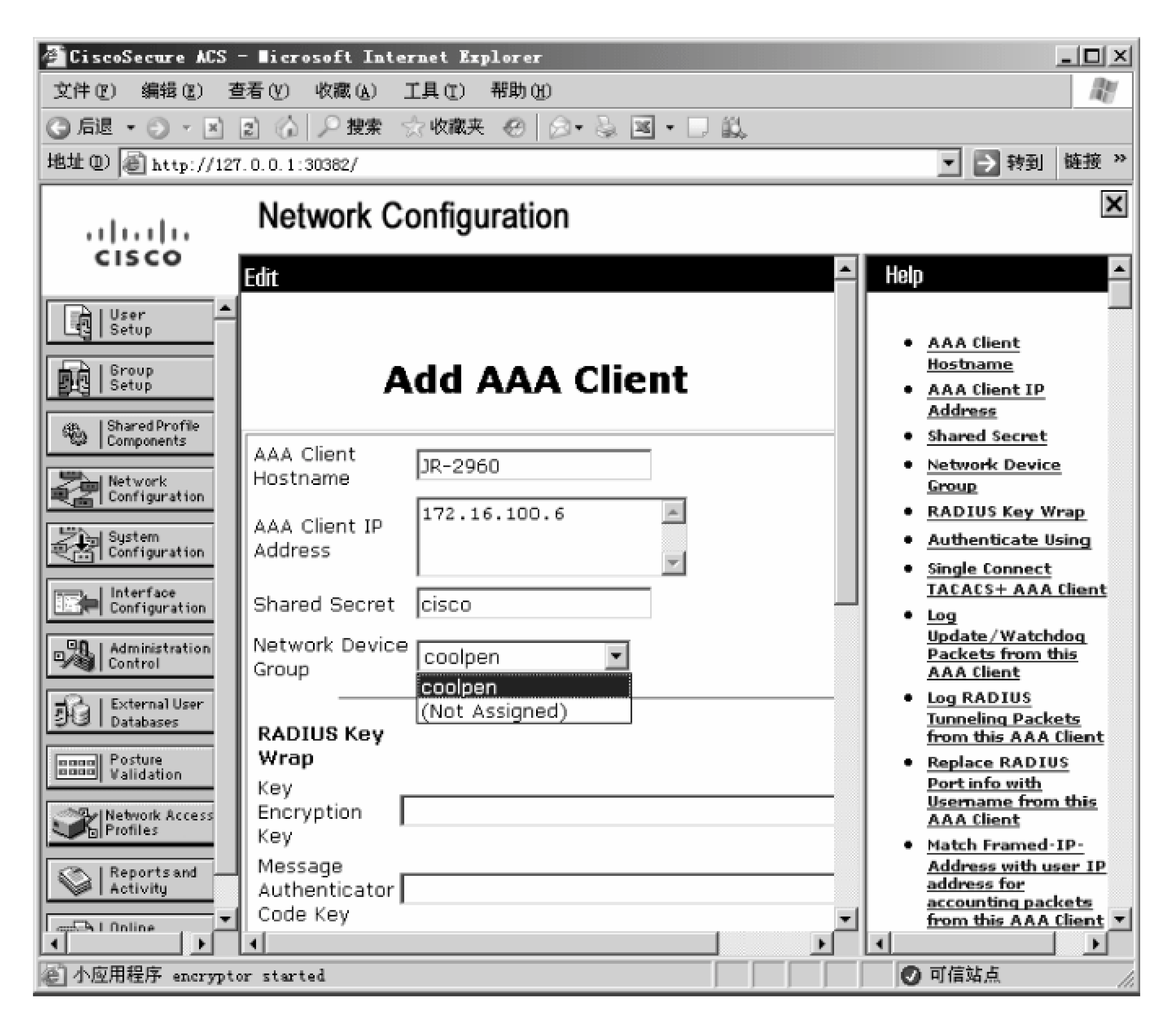


图 8-36　Add AAA Client 窗口

客户端的所有数据包，以便管理员随时查看用户登录情况，如图 8-37 所示。此处选择的身份验证方式必须与交换机端完全相同，即同时选择 RADIUS 身份验证方式。RADIUS 几乎是用于所有类型的网络设备，而 TACACS+仅适用于运行 Cisco IOS 的网络设备，这里选择的 RADIUS(IETF)是互联网领域通用的 RADIUS 身份验证技术。

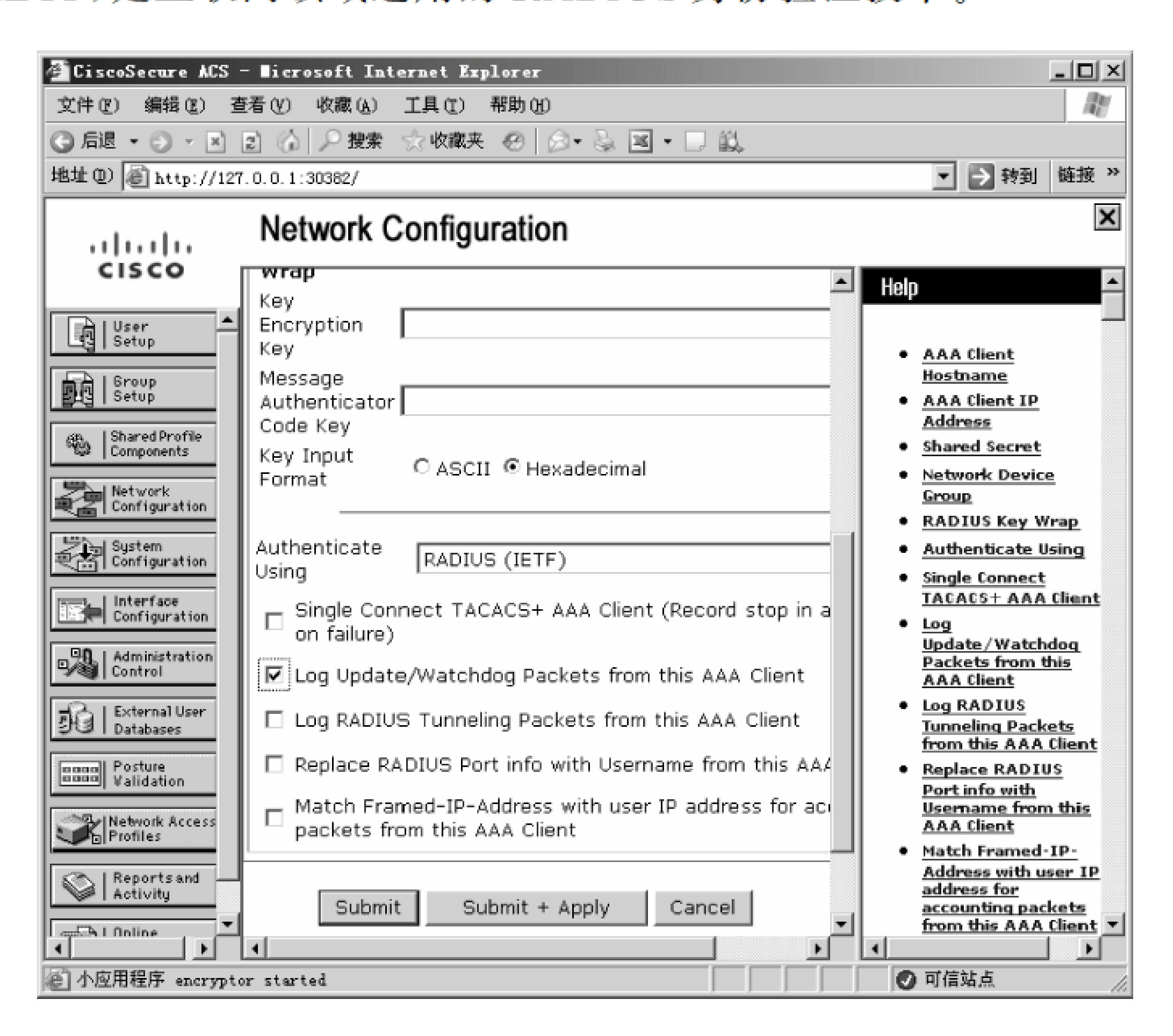


图 8-37　设置身份验证方式

（6）单击 Submit＋Apply 按钮，保存设置并返回 Network Configuration 窗口，JR-2960 就是刚刚创建的 AAA 客户端，如图 8-38 所示。

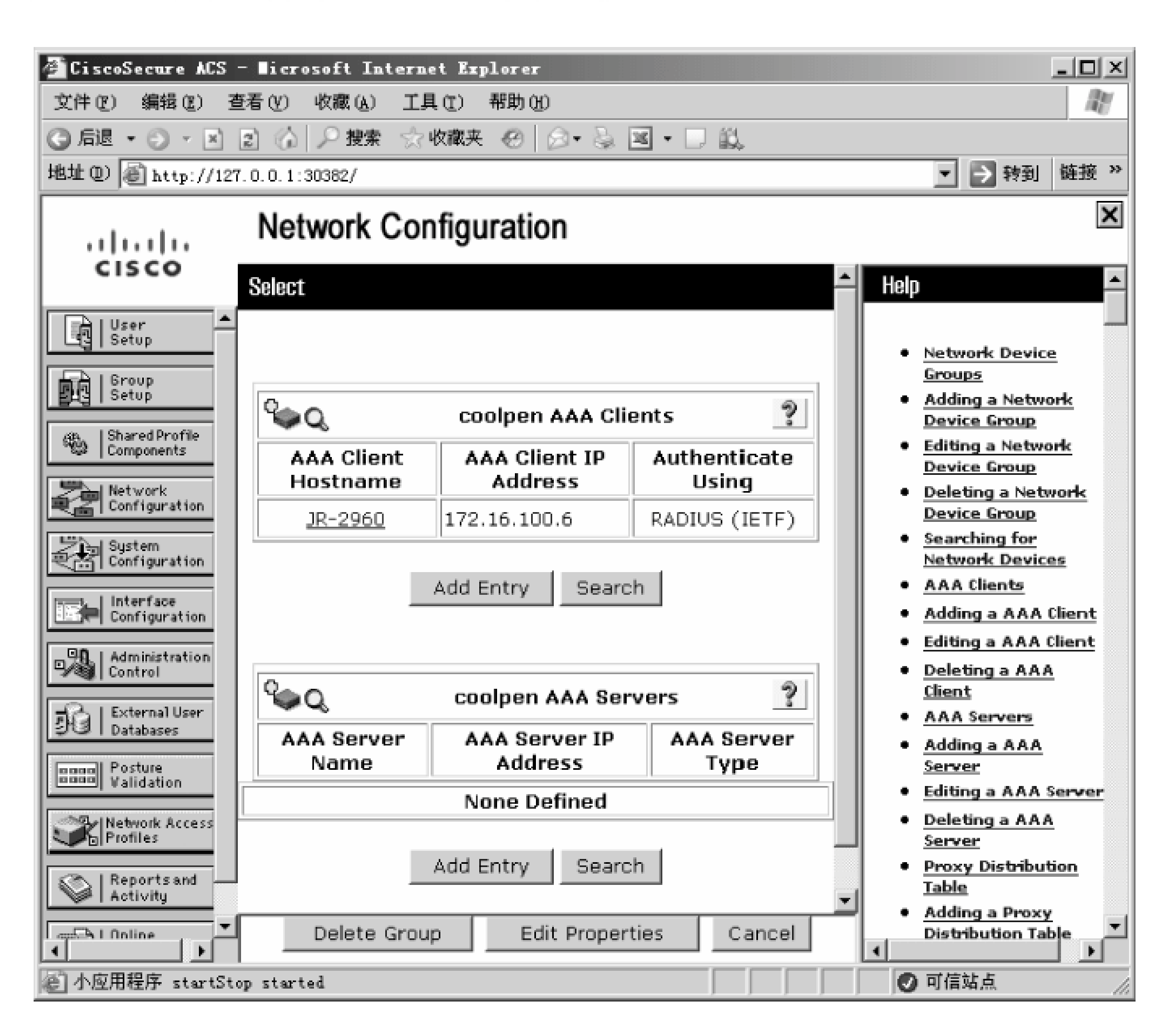


图 8-38　成功创建 AAA 客户端

（7）在 coolpen AAA Servers 选项区域内单击 Add Entry 按钮，显示如图 8-39 所示的 Add AAA Server 窗口。在 AAA Server Name 文本框中输入 AAA 服务器的名称，即 ACS 服务器的名称；在 AAA Server IP Address 文本框中输入 ACS 服务器的 IP 地址；在 Key

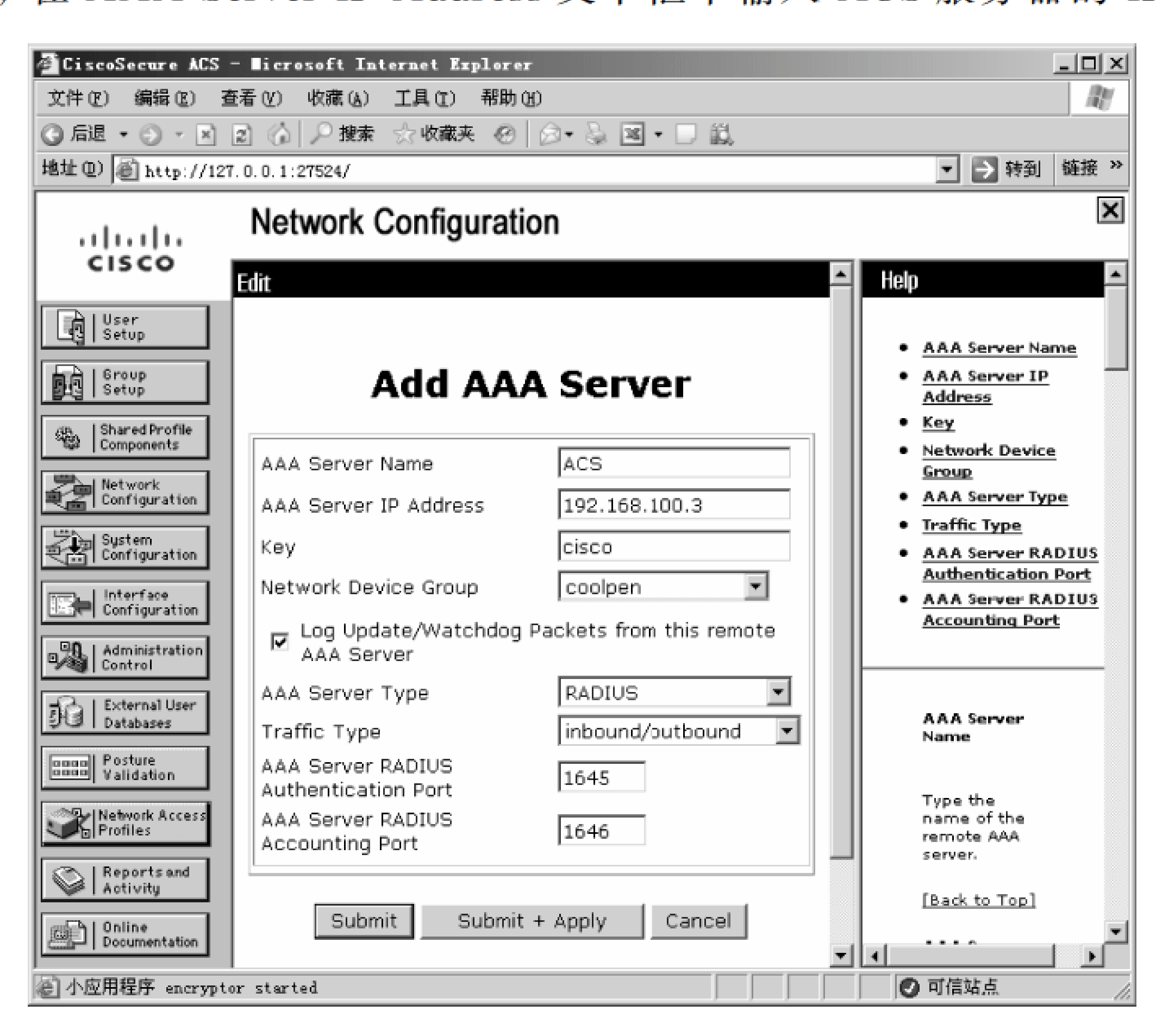


图 8-39　Add AAA Server 窗口

文本框中输入与交换机端配置完全相同的共享密钥；在 AAA Server Type 下拉列表框中选择 RADIUS 选项；在 Traffic Type 下拉列表框中选择 inbound/outbound 选项；保留默认的通信端口设置即可。

(8) 单击 Submit+Apply 按钮，保存设置。

3. 用户计算机配置

用户计算机的配置步骤如下。

(1) 启动 802.1x 身份验证客户端功能。打开“服务”窗口，右击 Wired AutoConfig 服务并选择快捷菜单中的“启动”命令，启动该服务，如图 8-40 所示。如果希望此服务随系统自动启动，则可以将其启动类型修改为“自动”。另外，还要确保 Extensible Authentication Protocol 服务处于“启动”状态。

(2) 打开“网络连接”窗口，右击正在使用的本地连接(例如“本地连接”)并选择快捷菜单中的“属性”命令，显示“本地连接 属性”对话框，单击“身份验证”标签切换到如图 8-41 所示的“身份验证”选项卡。选中“启用 IEEE 802.1x 身份验证”和“缓存用户信息以便随后连接网络使用”复选框。



图 8-40 启动相关服务

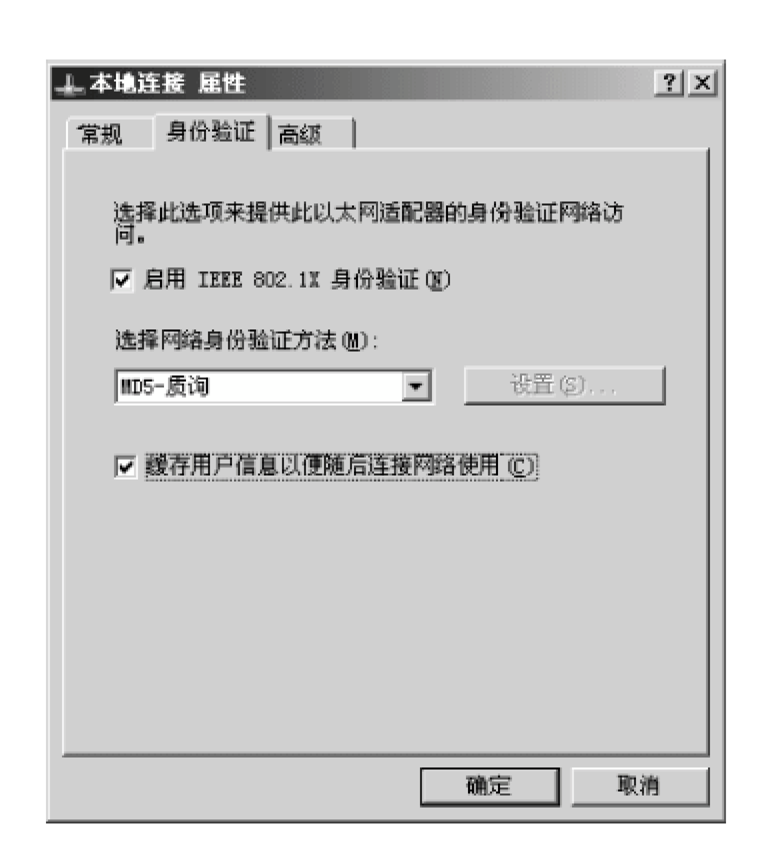


图 8-41 “身份验证”选项卡

(3) 单击“确定”按钮，保存配置。

4. 登录测试

(1) 网络用户完成计算机配置之后，即可开始向交换机发送身份验证请求，任务栏中的图标显示如图 8-42 所示的状态，配置 802.1x 身份验证之前，网络连接是断开的。

(2) 当任务栏显示“需要其他信息以连接到网络”提示信息时，单击提示信息显示如图 8-43 所示的“输入凭据”对话框。输入被 ACS 服务器授予访问权限的用户账户和密码，例如 user。

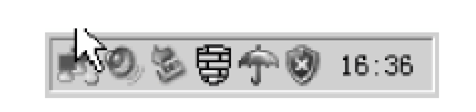


图 8-42 尝试连接到网络

(3) 单击“确定”按钮，向交换机发送身份验证信息，交换机将身份验证请求转发到 ACS 服务器，如果通过 ACS 服务器身份验证，则成功建立网络连接，任务栏中的图标显示如图 8-44 所示的状态。



图 8-43　“输入凭据”对话框

图 8-44　成功连接到网络

8.4.2　无线 AP 的 802.1x 认证

通过为无线 AP 配置 802.1x 身份验证，可以对通过无线 AP 接入企业网络的用户计算机进行身份验证，以确认是否允许其访问网络。无线客户端尝试访问无线 AP 时，首先无线 AP 会将用户提交的身份验证信息发送到网络中的 ACS 服务器，然后由 ACS 服务器根据用户账户赋予用户对应的权限。

1. 无线 AP 的配置

（1）初始化无线 AP

为了便于配置和管理无线 AP，首先应为无线 AP 配置主机名、IP 地址和子网掩码等信息。

① 进入全局配置模式。

```
ap# configure terminal
```

② 设置无线 AP 的主机名。

```
ap(config)# hostname AP
```

③ 指定要配置的接口。

```
AP(config)# interface fastEthernet 0
```

④ 设置接口的 IP 地址和子网掩码。

```
AP(config-if)# ip address 192.168.4.253 255.255.255.0
```

⑤ 启用该端口。

```
AP(config-if)# no shutdown
```

⑥ 退出接口配置模式。

```
AP(config-if)# exit
```

⑦ 设置管理员账户，包括用户名、密码、权限级别等，用于 Web 管理。

```
AP(config)# username cisco privilege 15 password cisco
```

⑧ 启用 Web 管理方式。

AP(config)# ip http server

⑨ 指定 http 连接授权方式。

AP(config)# ip http authentication local

⑩ 进入接口配置模式。

AP(config)# interface dot11Radio 0

⑪ 启用端口。

AP(config-if)# no shutdown

（2）使用 Web 方式配置无线 AP

使用 Web 方式配置无线 AP 的操作步骤如下。

① 在 IE 浏览器地址栏中输入无线 AP 的管理地址 192.168.4.253，显示如图 8-45 所示的“连接到 192.168.4.253”对话框，输入初始化时创建的用户账户和密码。



图 8-45 “连接到 192.168.4.253”对话框

② 单击“确定”按钮，打开无线 AP 的 Web 管理窗口，单击 EXPRESS SECURITY 链接，显示如图 8-46 所示的 Express Security Set-Up 窗口。在 SSID 文本框中输入无线网络的 SSID 名称，在 Security 选项区域内选中 EAP Authentication 单选按钮，输入 RADIUS 服务器的名称和共享密钥，这里使用 ACS 服务器作认证，输入 ACS 服务器的 IP 地址和预定的共享密钥即可。

③ 单击窗口下方的 Apply 按钮，显示如图 8-47 所示的对话框，单击“确定”按钮即可保存设置。

2. ACS 服务器的配置

在 ACS 服务器上，首先应将无线 AP 配置为 ACS 客户端，然后配置网络用户连接到网络的用户账户信息。

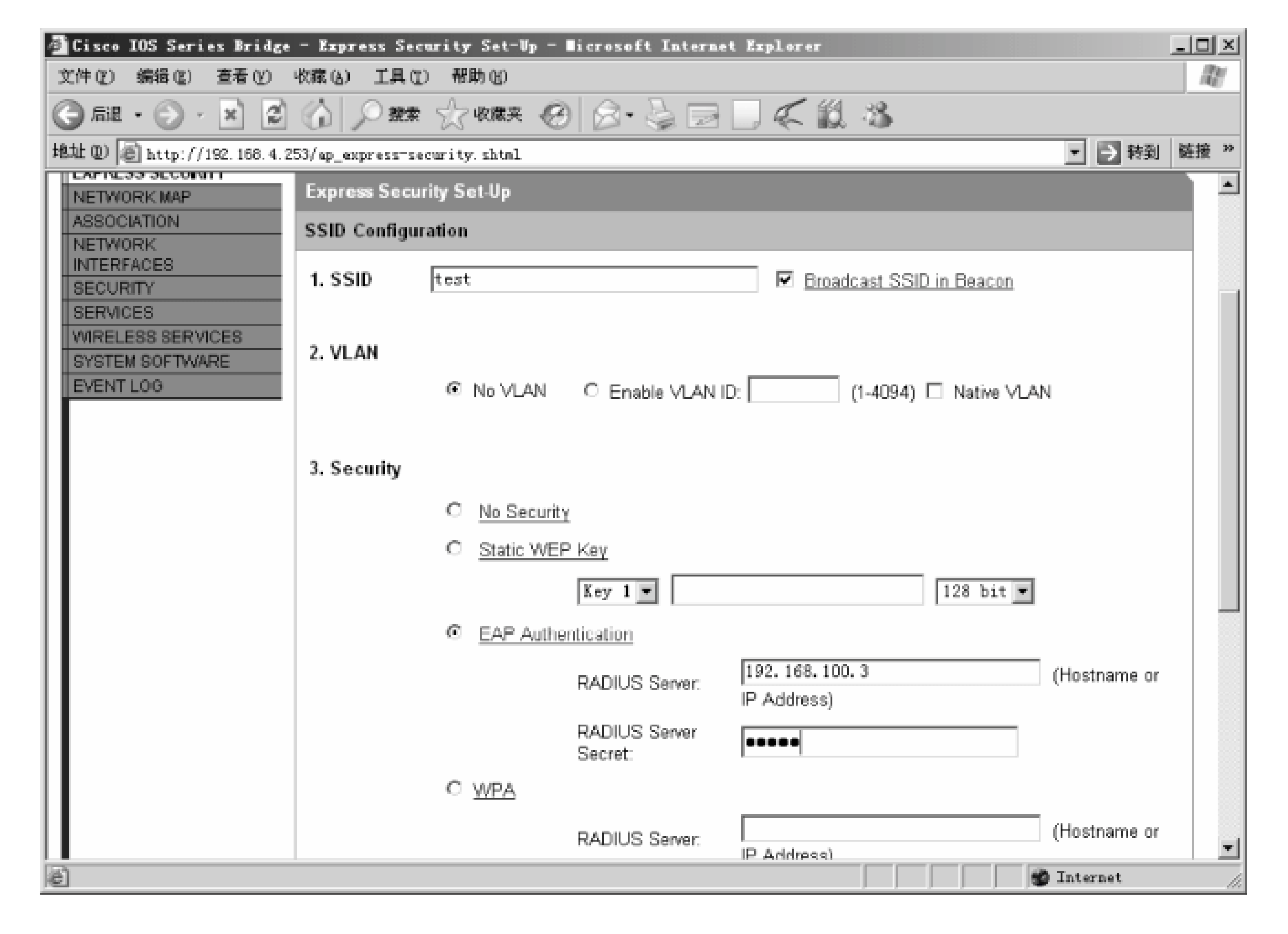


图 8-46　Express Security Set-Up 窗口



图 8-47　是否保存当前设置

（1）在 ACS 管理窗口中，单击 Network Configuration 按钮，显示如图 8-48 所示的窗口，创建 ACS 客户端组或者选择已有客户端组，这里选择在原有的 coolpen 组中创建 ACS 客户端。在 Network Device Group 选项区域内单击 coolpen 组，显示 coolpen AAA Clients 窗口。

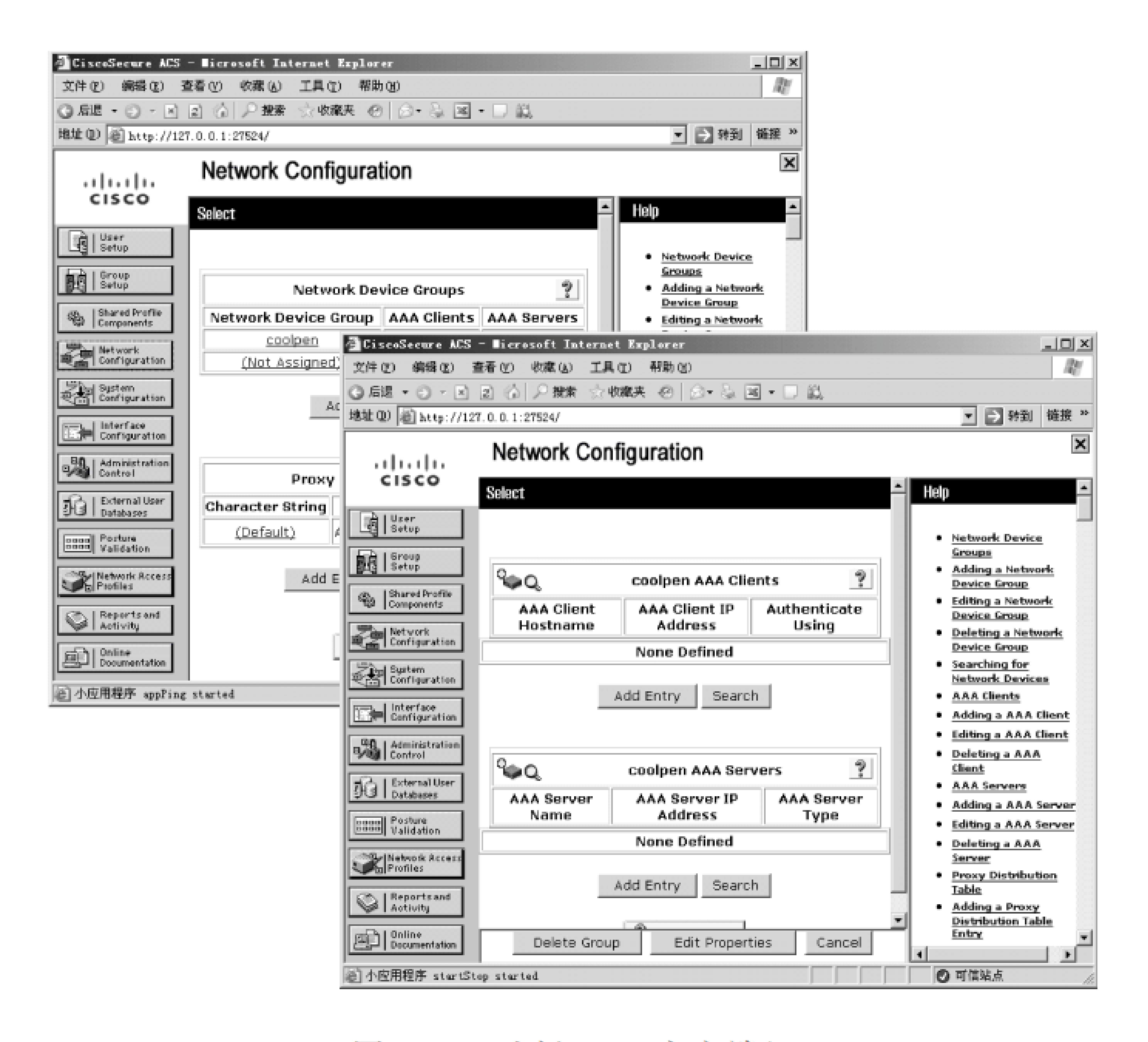


图 8-48　选择 ACS 客户端组

（2）单击 Add Entry 按钮，显示如图 8-49 所示的 Add AAA Client 窗口，在 AAA Client Hostname 文本框中输入无线 AP 的主机名，在 AAA Client IP Address 文本框中输

入无线 AP 的 IP 地址，在 Shared Secret 文本框中输入共享密钥(必须与无线 AP 的配置完全相同)，在 Network Device Group 下拉列表框中选择将该客户端指定到的分组，选择 coolpen 选项即可。

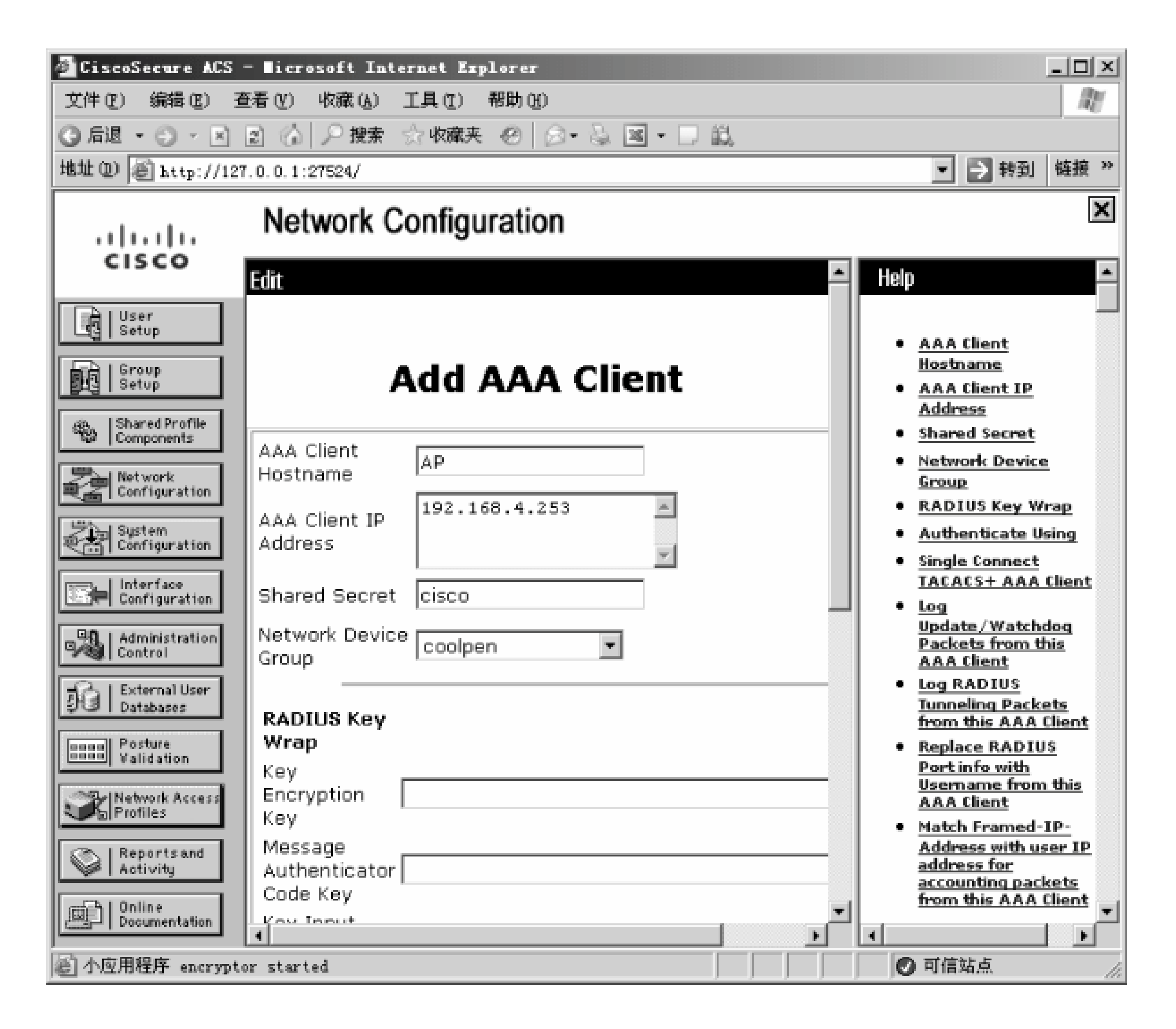


图 8-49　Add AAA Client 窗口

(3) 设置身份验证方式。向下拖动滚动条，在 Authenticate Using 下拉列表框中选择 RADIUS (Cisco Aironet)选项，同时选中 Log Update/Watchdog Packets from this AAA Client 复选框，记录来自 AAA 客户端的所有数据包，以便管理员随时查看用户登录情况，如图 8-50 所示。

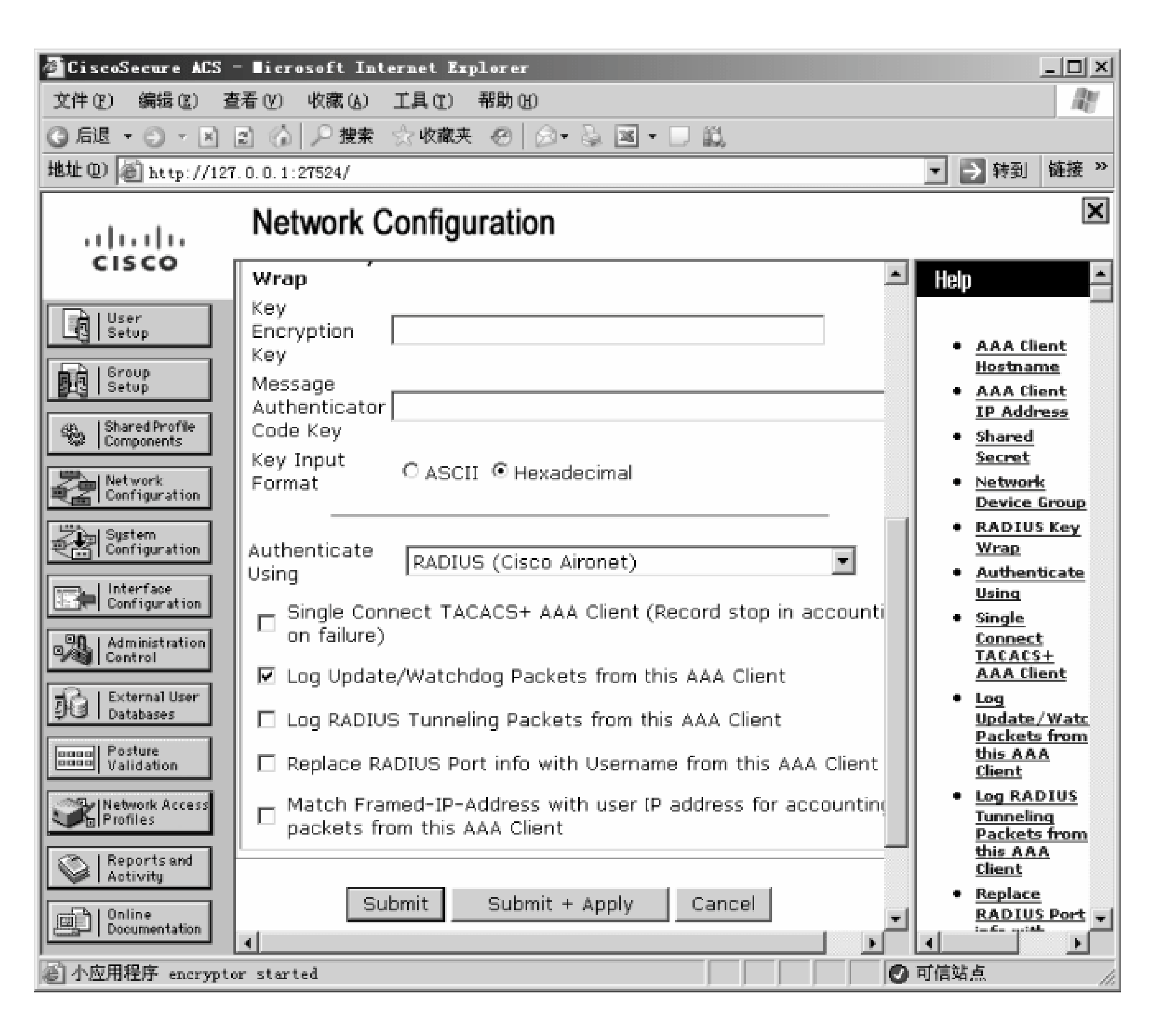


图 8-50　设置身份验证方式

（4）单击 Submit+Apply 按钮保存设置。接下来还要设置用户账户和密码，与“基于ACS 的基本认证”中的配置基本相同，此处不再赘述。

3. 用户计算机配置

客户端计算机默认并未启用 802.1x 身份验证功能，若想连接到启用 802.1x 身份验证的无线 AP，必须进行如下配置。

（1）在“网络连接”窗口中，右击“无线网络连接”并选择快捷菜单中的“属性”命令，显示如图 8-51 所示的“无线网络连接 属性”对话框，切换到“无线网络配置”选项卡。

（2）单击“查看无线网络”按钮，显示如图 8-52 所示的“无线网络属性”对话框，在“关联”选项卡中，输入无线网络的 SSID 名称，必须与无线 AP 的配置完全相同。

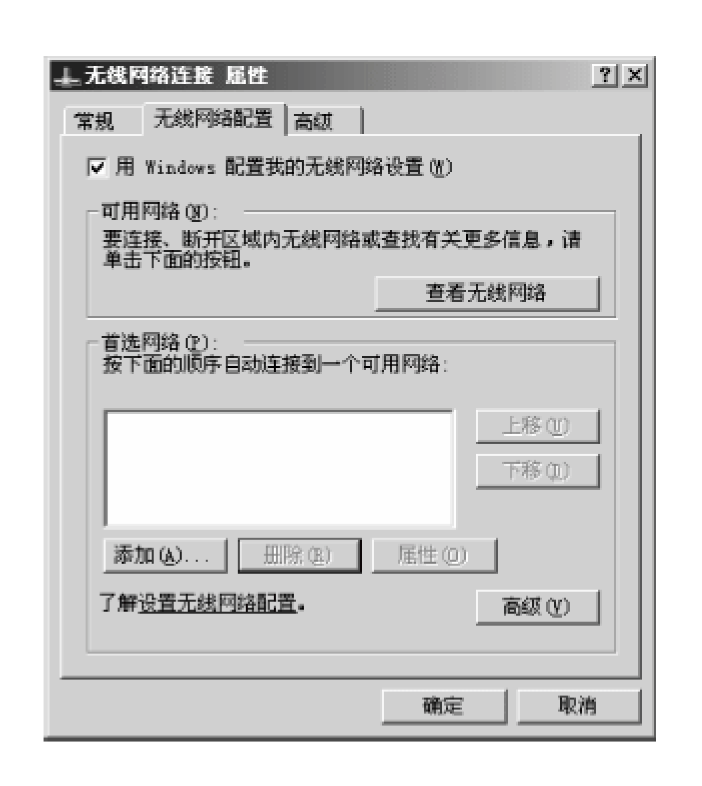





图 8-51　“无线网络连接 属性”对话框　　图 8-52　“无线网络属性”对话框

（3）单击“验证”标签，切换到如图 8-53 所示的“验证”选项卡，选中“启用此网络的IEEE 802.1x 验证”复选框，在“EAP 类型”下拉列表框中选择“受保护的 EAP(PEAP)”选项，必须与无线 AP 的配置完全相同，取消“当计算机信息可用时验证为计算机”复选框。

（4）单击“属性”按钮，显示如图 8-54 所示的“受保护的 EAP 属性”对话框，取消“验证服务器证书”复选框，在“选择验证方法”下拉列表框中选择“安全密码(EAP-MSCHAP v2)”选项。

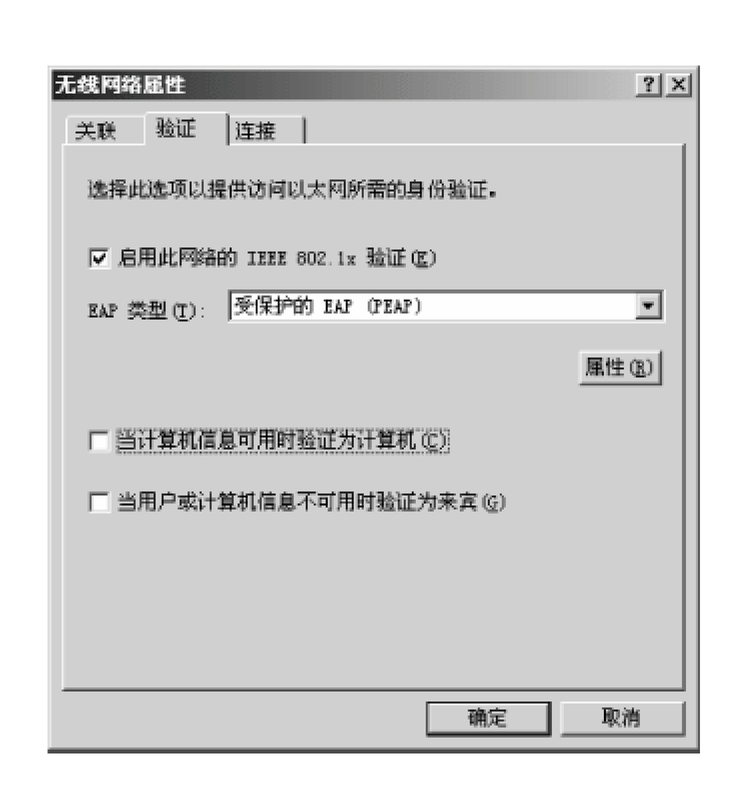




图 8-53　“验证”选项卡　　图 8-54　“受保护的 EAP 属性”对话框

（5）单击“配置”按钮，显示如图 8-55 所示的“EAP MSCHAPv2 属性”对话框，取消“自动使用 Windows 登录名和密码(以及域，如果有的话)”复选框。

4. 登录测试

登录测试的具体操作步骤如下。

(1) 用户计算机完成基本配置后,任务栏中的无线网络连接将提示如图 8-56 所示的信息,要求提供凭据才可以连接到指定的无线网络。

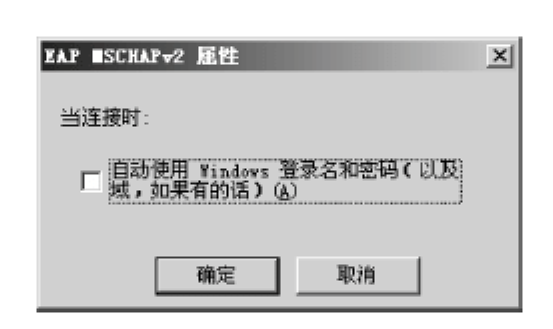


图 8-55 “EAP MSCHAPv2 属性”对话框

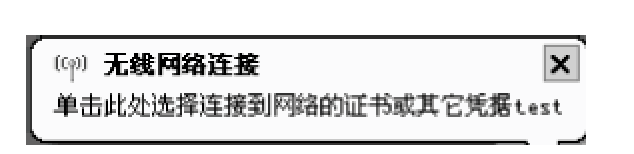


图 8-56 提示需要凭据

(2) 单击提示信息,显示如图 8-57 所示的“输入凭据”对话框,输入用户名和密码,单击“确定”按钮,将用户信息发送到无线 AP,无线 AP 将身份验证信息发送到 ACS 服务器进行身份验证。

(3) 成功连接到无线 AP 后,显示如图 8-58 所示的对话框,test 就是启用 802.1x 身份验证的无线 AP。

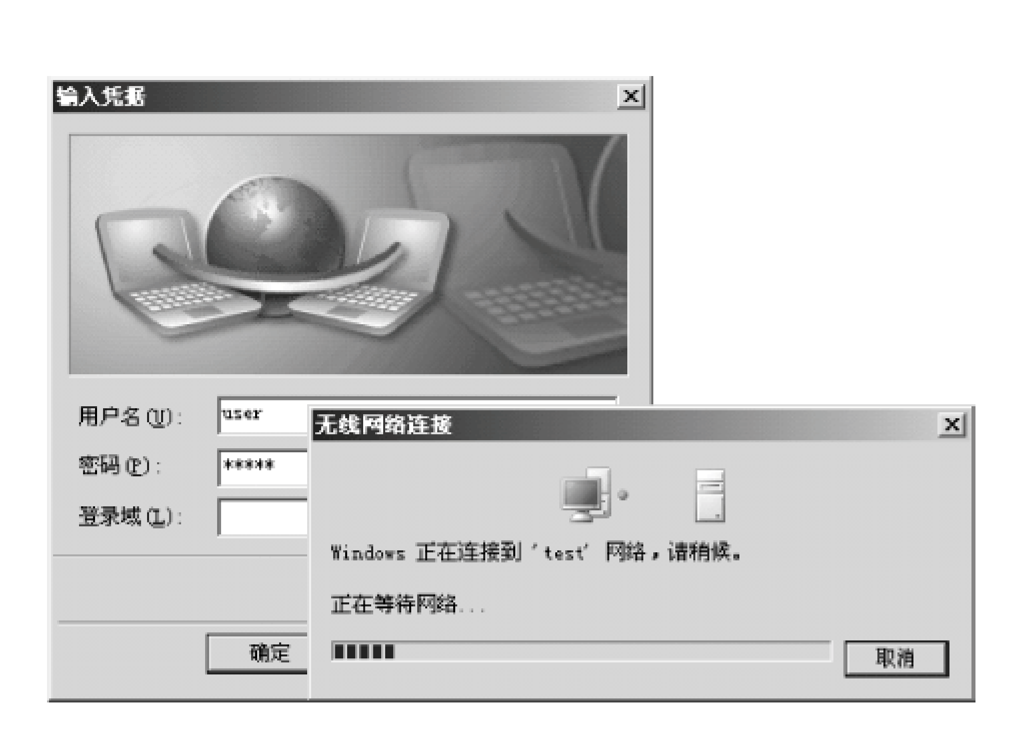


图 8-57 “输入凭据”对话框

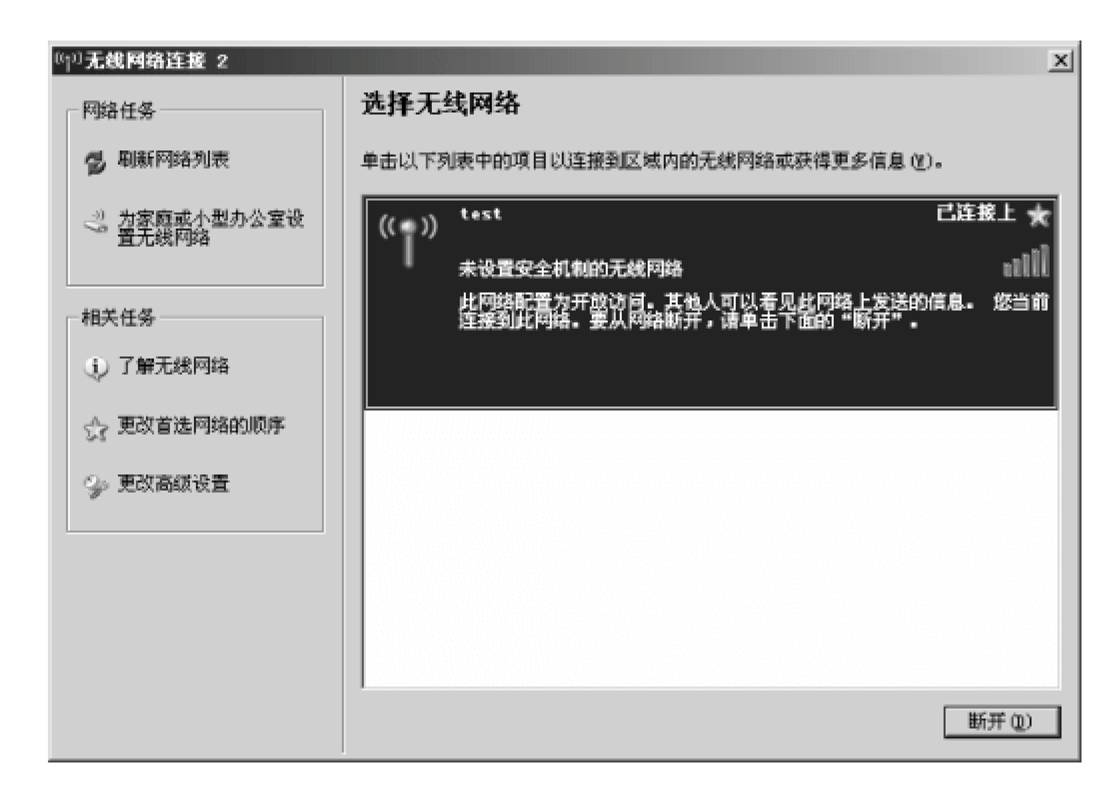


图 8-58 成功连接到无线 AP

8.4.3 知识链接:IEEE 802.1x

以太网技术“连通和共享”的设计初衷使目前由以太网构成的网络系统面临着很多安全问题。IEEE 802.1x 协议正是在基于这样的背景下被提出来的,成为解决局域网安全问题的一个有效手段。

在 IEEE 802.1x 协议中,只有具备了以下 3 个元素(如图 8-59 所示)才能够完成基于端口的访问控制的用户认证和授权。

(1) 客户端。一般安装在用户的工作站上,当用户有上网需求时,激活客户端程序,输入必要的用户名和口令,客户端程序将会送出连接请求。

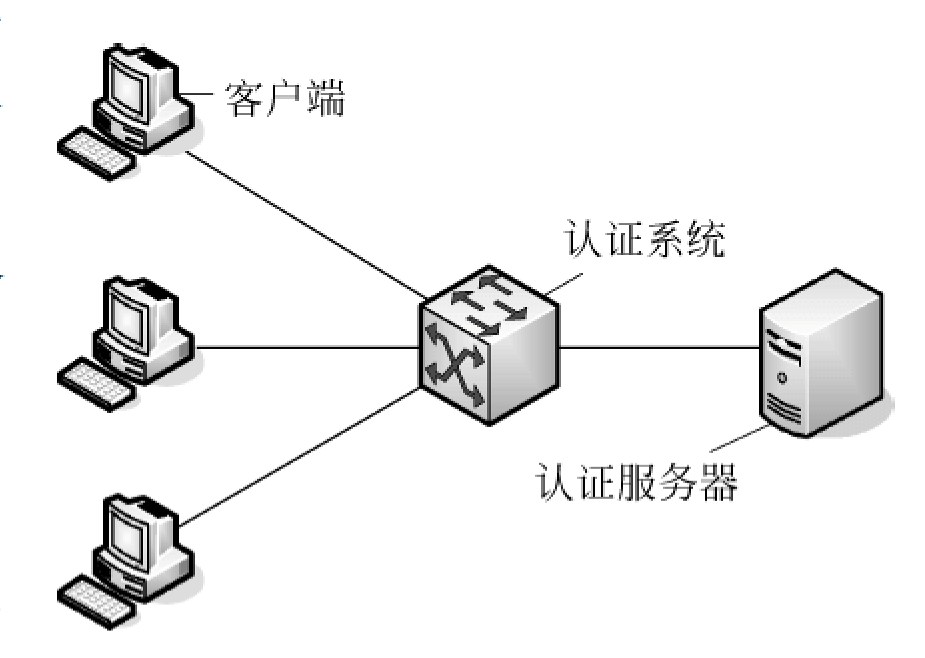


图 8-59 IEEE 802.1x 协议认证三要素

(2) 认证系统。在以太网系统中指认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。

(3) 认证服务器。通过检验客户端发送来的身份标识(用户名和口令)来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的状态。

在具有 802.1x 认证功能的网络系统中，当一个用户需要对网络资源进行访问之前必须先要完成以下认证过程(如图 8-60 所示)。

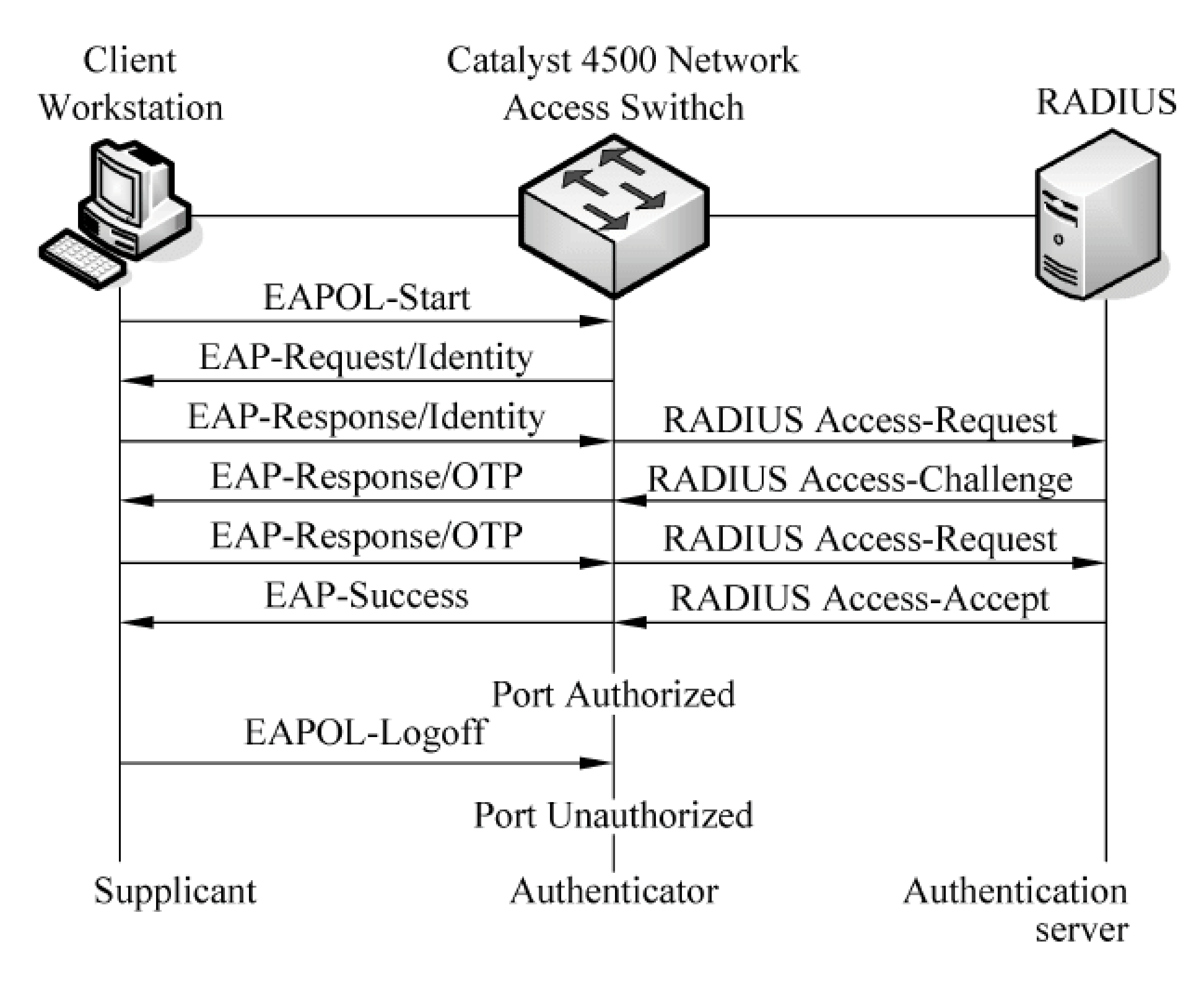


图 8-60　802.1x 认证过程

(1) 当用户有上网需求时打开 802.1x 客户端程序，输入已经申请、登记过的用户名和口令，发起连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

(2) 交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名送上来。

(3) 客户端程序响应交换机发出的请求，将用户名信息通过数据帧送给交换机。交换机将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

(4) 认证服务器收到交换机转发上来的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。

(5) 客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密处理(此种加密算法通常是不可逆的)，并通过交换机传给认证服务器。

(6) 认证服务器将送上来的加密后的口令信息和自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向交换机发出打开端口的命令，允许用户的业务流通过端口访问网络。否则，反馈认证失败的消息，并保持交换机端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

习题

1. 简述 CiscoSecure ACS 的主要应用环境。
2. CiscoSecure ACS 服务器的功能有哪些?
3. 基于 Active Directory 的 ACS 服务器相对于其他方式有哪些优点?
4. 什么是 802.1x 身份验证?
5. 简述 802.1x 身份验证的实现机制。

实验:借助 ACS 实现交换机 802.1x 身份验证

实验目的:

运用 CiscoSecure ACS+Active Directory 实现 802.1x 身份验证。

实验内容:

使用 CiscoSecure ACS 与 Windows Server 2008 系统的 Active Directory 相结合,为交换机实现 802.1x 身份验证。

实验步骤:

(1) 准备 CiscoSecure ACS 所需的网络环境,将 ACS 服务器及其所需的其他成员服务器和客户端连接在交换机上,组成一个子网,并测试彼此之间的连通性。

(2) 部署 ACS 服务器。

(3) 在域控制器上创建用于测试的用户账户和组。

(4) 建立 ACS 服务器和域控制器之间的关联。

(5) 将交换机配置 ACS 服务器的 AAA 客户端。

(6) 登录交换机并启用其 802.1x 身份验证功能,建立其到 ACS 服务器的连接。

(7) 在 ACS 服务器上为测试用户账户授权,配置允许其运行的管理命令。

(8) 在客户端计算机上尝试 Telnet 登录交换机,验证配置是否生效。

第 9 章 chapter 9

Internet接入安全

网络防火墙是企业网络必不可少的安全防御措施，例如部署在局域网出口处的 Cisco ASA 5540、客户端计算机的 Windows 防火墙等。美中不足的是，这些防火墙缺少统一的管理机制，很难实现服务器和客户端之间的协同工作。Forefront TMG(Threat Management Gateway)是 Microsoft Forefront 系列中的产品之一，是 ISA Server 的升级版本。Forefront TMG 不仅提供分布式防火墙功能，而且还提供代理服务器和 Web 缓存等实用功能，可以有效控制网络内部与外部的通信，防范外来网络的攻击，提高网络性能和安全性。

9.1 Internet 接入安全规划

Internet 接入安全是网络安全防御的重要目标。企业网络的所有客户端和网络设备均通过该接口接入 Internet，而来自外网的所有攻击和威胁因素也均由此接口进入，其重要性可见一斑，这也是在此处部署硬件防火墙的主要原因。除此之外，还应部署一套基于软件的应用层安全防御系统，来加强网络安全管理。

9.1.1 案例情景

目前，该企业局域网的出口处已经部署了集成 VPN 功能 Cisco ASA 5540 硬件防火墙，可以提供基本的远程安全接入和 Internet 安全接入。但是无法对网络客户端用户的应用进行严格限制，致使网络统一管理难以实施。例如，无法限制客户端用户在工作时间内聊天、浏览视频网站，无法对客户端下载文件进行监控，进而导致病毒程序的全网泛滥。

9.1.2 项目需求

企业网络中的客户端和服务器，大部分使用 Microsoft 的 Windows 产品，如果用来自其他厂商的安全解决方案来保护当前网络，很容易出现兼容性问题。因此，应尽量采用 Microsoft 公司的安全产品，Forefront TMG 是 Microsoft 最新推出的网络边缘安全产品，可以同时为企业网络中的服务器和客户端提供安全保护，适用范围更广，并且允许用户针对不同的环境需求，配置不同的网络策略，可以灵活控制内部客户端访问 Internet 的行为。

9.1.3 解决方案

Forefront TMG 服务器不仅可以解决企业网络应用层安全产品缺失的问题，而且可以

满足企业网络未来一段时间发展的需求，具有很强的并发访问支持能力。TMG 提供多种网络应用模板，以适应不同的网络需要，例如边缘防火墙、3 向外围网络防火墙、前端防火墙、后端防火墙以及单一网络适配器防火墙。当前企业网络中，Forefront TMG 代理服务器接入只是路由器接入和防火墙接入的一种替代方案，可以将 Forefront TMG 服务器直接部署在网络边缘，图 9-1 所示为 TMG 服务器的部署示意图

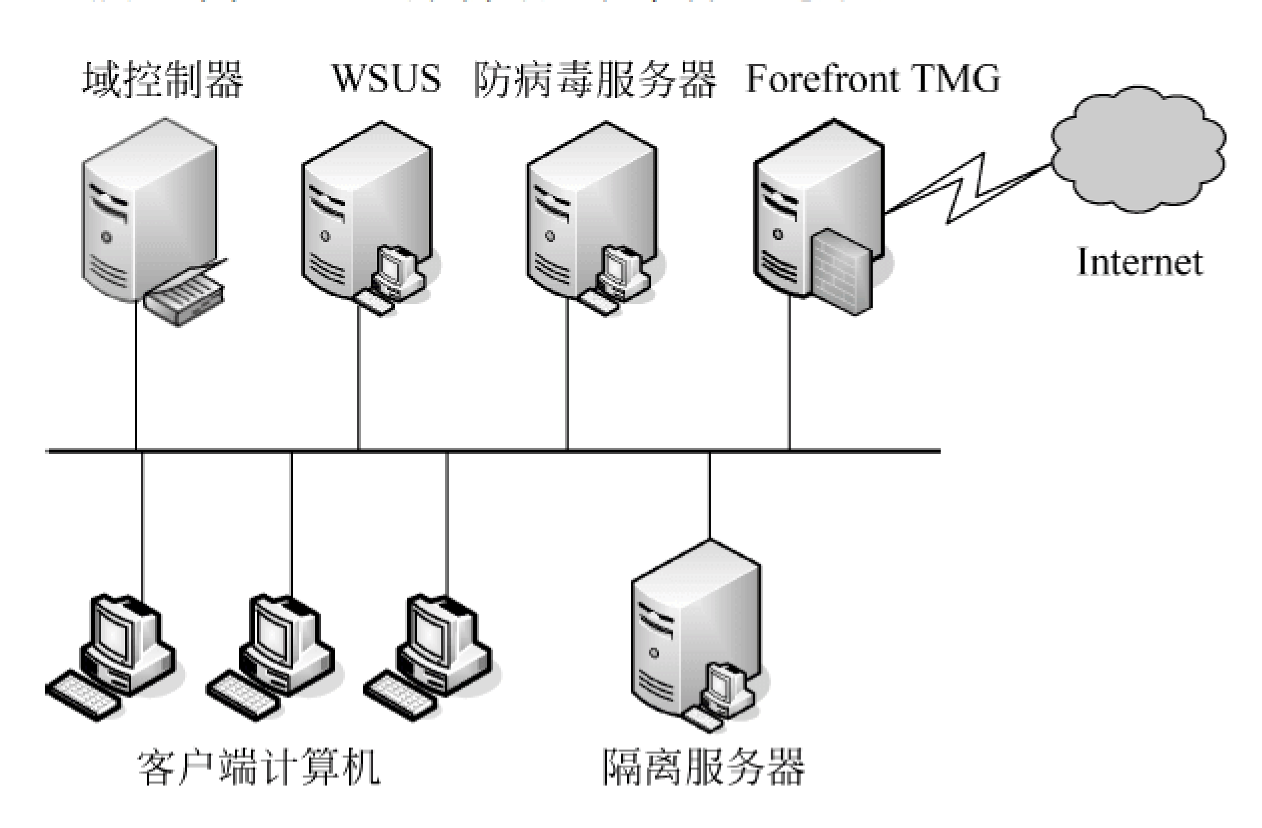


图 9-1 TMG 服务器的部署示意图

本章中 TMG 服务器运行 Windows Server 2008 操作系统。TMG 服务器使用域管理员身份登录。如果为 TMG 服务器建立独立账号，需要将该账号添加到 TMG 服务器的本地管理员组中。

9.2 安装 Forefront TMG 服务器

Forefront TMG 具有 ISA Server 所提供的所有功能，除了代理服务器提供共享上网、担任防火墙保护内部网络安全以及利用 Web 缓存增加访问速度以外，还可以搭建 VPN 服务器，提供远程安全访问。另外，还增加了恶意软件检查功能，杜绝 Internet 访问中的病毒和间谍软件，从而大大提供局域网访问 Internet 时的安全性。

9.2.1 安装需求

Forefront TMG 对服务器的软件和硬件环境都有一定的要求，而且所连接的客户端越多，所要求的配置也越高。不过，安装时的要求并不高，只需满足以下条件即可。

(1) 服务器使用 1GHz 或更高 CPU。

(2) 服务器采用 Windows Server 2008 x64 操作系统。

(3) 1GB 内存或更高。

(4) Forefront TMG 服务器需要至少两块网络适配器，一块用于与内部网络通信；另一块用于连接外部网络。

(5) 磁盘分区采用 NTFS 文件系统，并且拥有至少 150MB 的可用空间。

(6) 数据库采用 Microsoft SQL Server 2005 Express Edition。

每台 Forefront TMG 服务大约(最大同时)能连接 500～1000 个客户端，如果企业中的

计算机更多，要想实现高性能、高安全性(在发生服务器硬件故障时不中断服务)，就需要利用 Forefront TMG 组成“阵列”方式。

9.2.2 安装 Forefront TMG

Forefront TMG 的安装过程很简单，完成所有准备工作之后即可开始安装。

(1) 运行 Forefront TMG 安装光盘，显示如图 9-2 所示的“Microsoft Forefront TMG 安装程序”窗口。

(2) 单击“安装 Forefront TMG”链接，运行安装向导。连续单击“下一步”按钮，在“客户信息”对话框中输入用户名、单位和产品序列号；在“安装方案”对话框中，选中“安装 Forefront Threat Management Gateway”单选按钮，如图 9-3 所示。






图 9-2 Forefront TMG 安装界面

图 9-3 “安装方案”对话框

(3) 连续单击“下一步”按钮，在“组件选择”对话框中选择欲安装的组件；在“内部网络”对话框中添加内部网络的地址。单击“添加”按钮，显示如图 9-4 所示的“地址”对话框，用来添加内部网络的 IP 地址范围。

如果要根据网卡添加，可单击“添加适配器”按钮，显示如图 9-5 所示的“选择网络适配器”对话框，选择连接内部网络的网卡，即可自动添加相应的 IP 地址段。

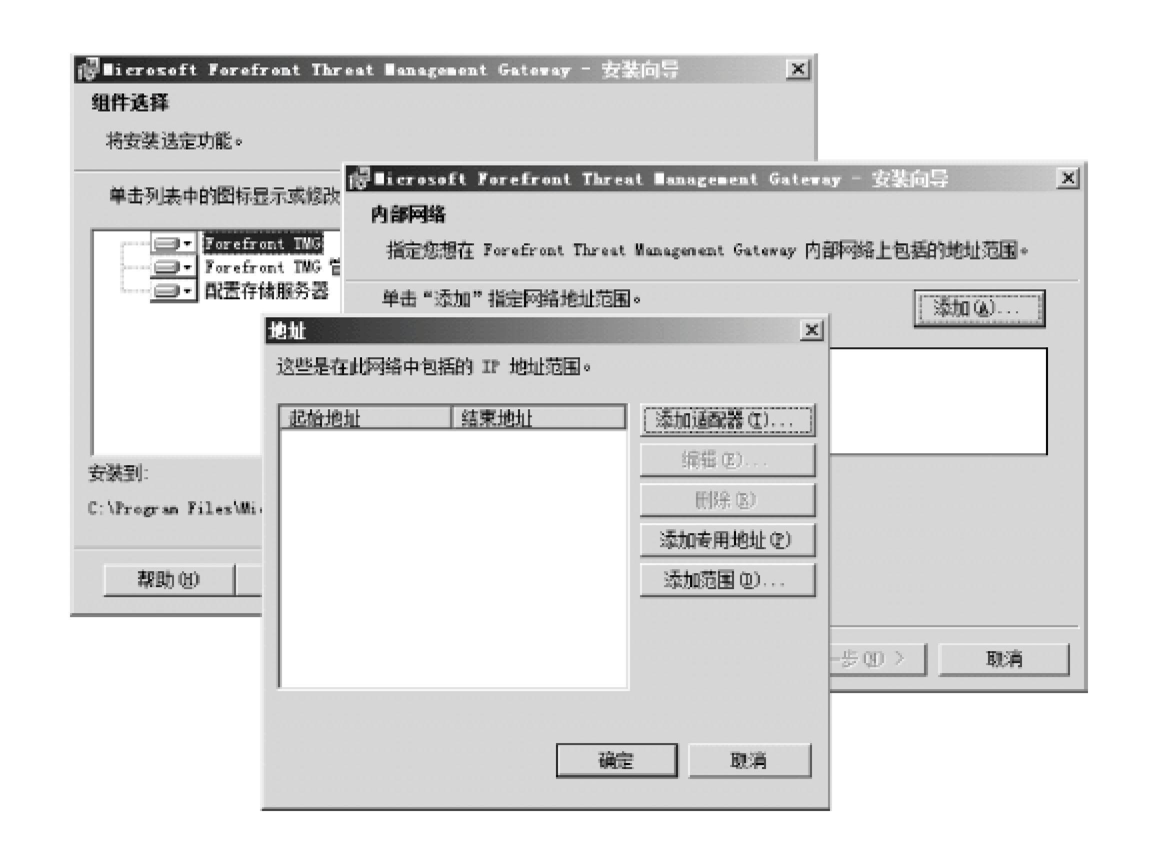


图 9-4 添加地址范围

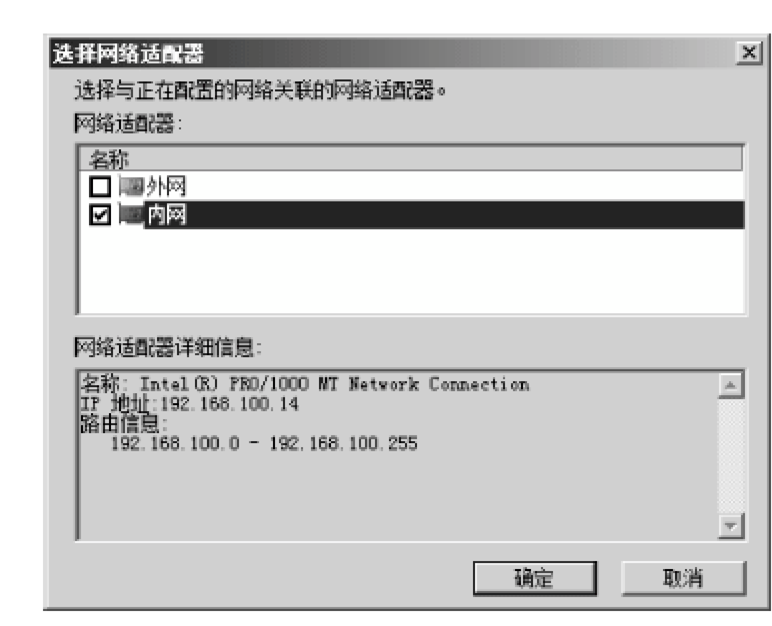


图 9-5 “选择网络适配器”对话框

如果网络内还包含有其他类型的 IP 地址段，可单击“添加专用地址”按钮，在下拉列表框中选择相应的私有 IP 地址段，如图 9-6 所示。

如果添加专门的 IP 地址段，可单击“添加范围”按钮，显示如图 9-7 所示的“IP 地址范围属性”对话框，输入起始地址和结束地址即可。



图 9-6　添加专用地址



图 9-7　“IP 地址范围属性”对话框

(4) 单击“确定”按钮返回“内部网络”对话框。单击“下一步”按钮，显示如图 9-8 所示的“服务警告”对话框，列出了在安装过程中将需要重新启动和停止的服务。

(5) 单击“下一步”按钮，显示“为安装程序做好准备”对话框。单击“安装”按钮即可开始安装。完成后显示“安装向导完成”对话框，Forefront TMG 安装完成，如图 9-9 所示。



图 9-8　“服务警告”对话框



图 9-9　Forefront TMG 安装完成

(6) 单击“完成”按钮退出安装向导，显示“保护 ISA 服务器计算机”窗口，并启动 Forefront TMG 控制台。首先会显示如图 9-10 所示的“入门向导”对话框，可用来简单而快速地配置 Forefront TMG，如果不运行向导，将其关闭即可。

(7) 在 Forefront TMG 控制台中展开服务器名，即可配置防火墙策略、网络策略及 VPN，如图 9-11 所示。也可以依次选择“开始”→“所有程序”→Microsoft Forefront TMG→“Forefront TMG 管理”，在右侧窗格的“任务”选项卡中，单击“启动入门向导”链接，也可以重新启动入门向导。



图 9-10　入门向导



图 9-11　Forefront TMG 控制台

9.3　配置 Forefront TMG

在第一次运行 Forefront TMG 时，会自动启动入门向导，可以完成配置网络设置、配置系统设置和定义部署选项，并可配置 Web 访问策略。不过，这 3 个向导是按顺序依次进行的，在首次使用时，必须先配置完前一个向导，才可配置下一个向导。而当配置完 Web 访问策略以后，局域网的计算机就可以直接访问 Internet 上的 Web 网站了。

9.3.1　配置网络设置

配置网络设置的操作步骤如下。

(1) 在“入门向导”对话框中单击“配置网络设置”链接，启动“入门-网络设置向导”。单击“下一步”按钮，显示“网络模板选择”对话框，用来选择最适合当前网络的拓扑结构，

如图 9-12 所示。

(2) 单击“下一步”按钮,显示“局域网(LAN)设置”对话框。在“连接到 LAN 的网络适配器”下拉列表框中,选择连接局域网的网络连接,如图 9-13 所示。

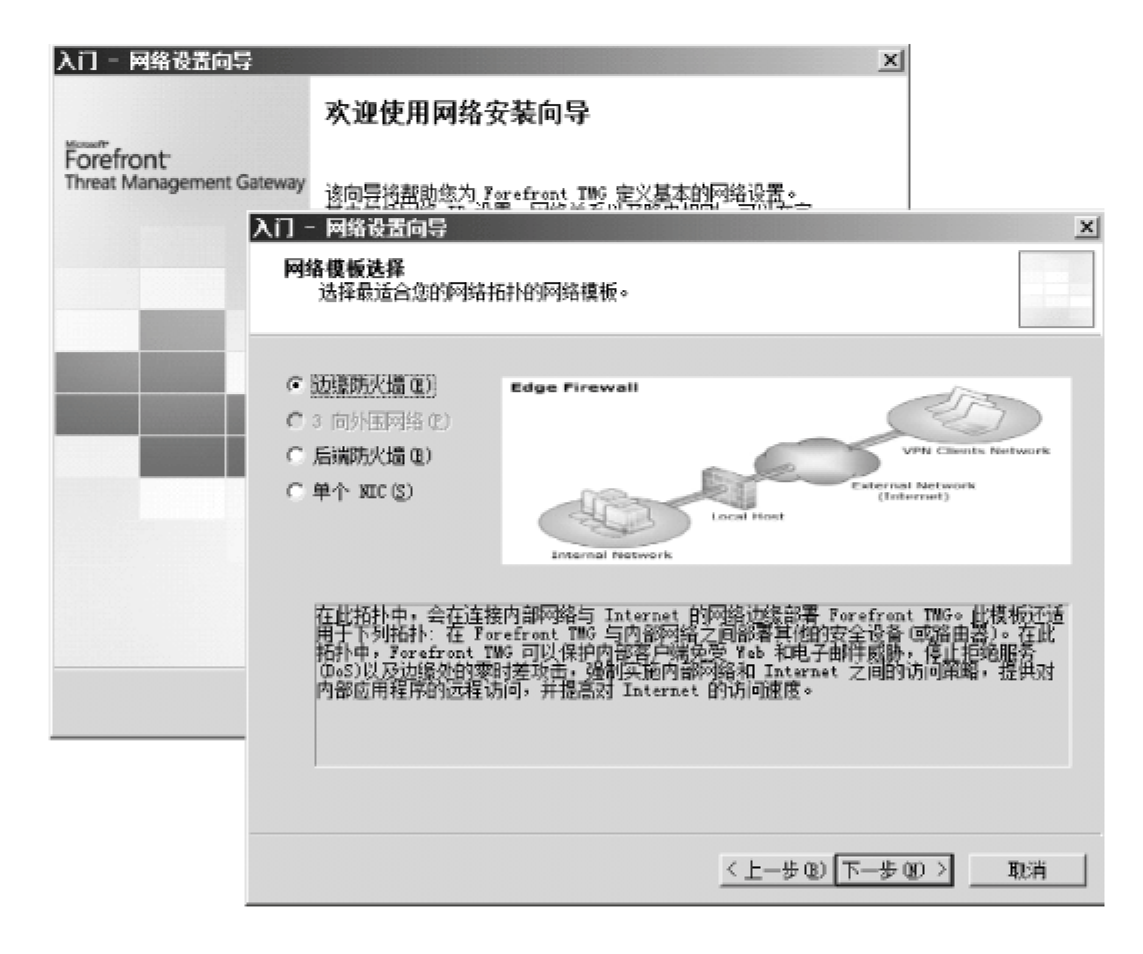


图 9-12 “网络模板选择”对话框

图 9-13 “局域网(LAN)设置”对话框

(3) 单击“下一步”按钮,显示“Internet 设置”对话框。在“连接到 Internet 的网络适配器”下拉列表框中,选择连接 Internet 的网络连接,如图 9-14 所示。

(4) 单击“下一步”按钮,网络设置向导完成,如图 9-15 所示。单击“关闭”按钮关闭即可。



图 9-14 “Internet 设置”对话框

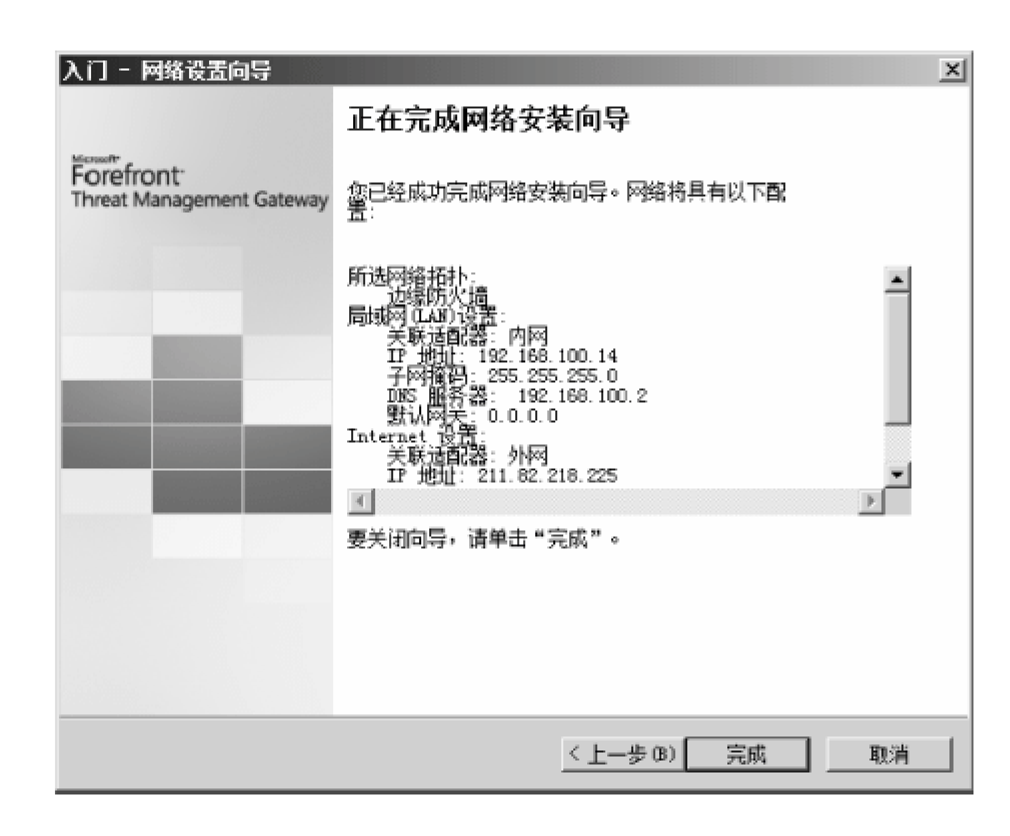


图 9-15 完成网络设置向导

9.3.2 配置系统设置

当“网络设置向导”完成以后,“配置系统设置”选项变为可用状态,可以用来定义本地系统设置了,如图 9-16 所示。

单击“配置系统设置”链接,启动“系统配置向导”。连续单击“下一步”按钮即可配置完成,如图 9-17 所示。

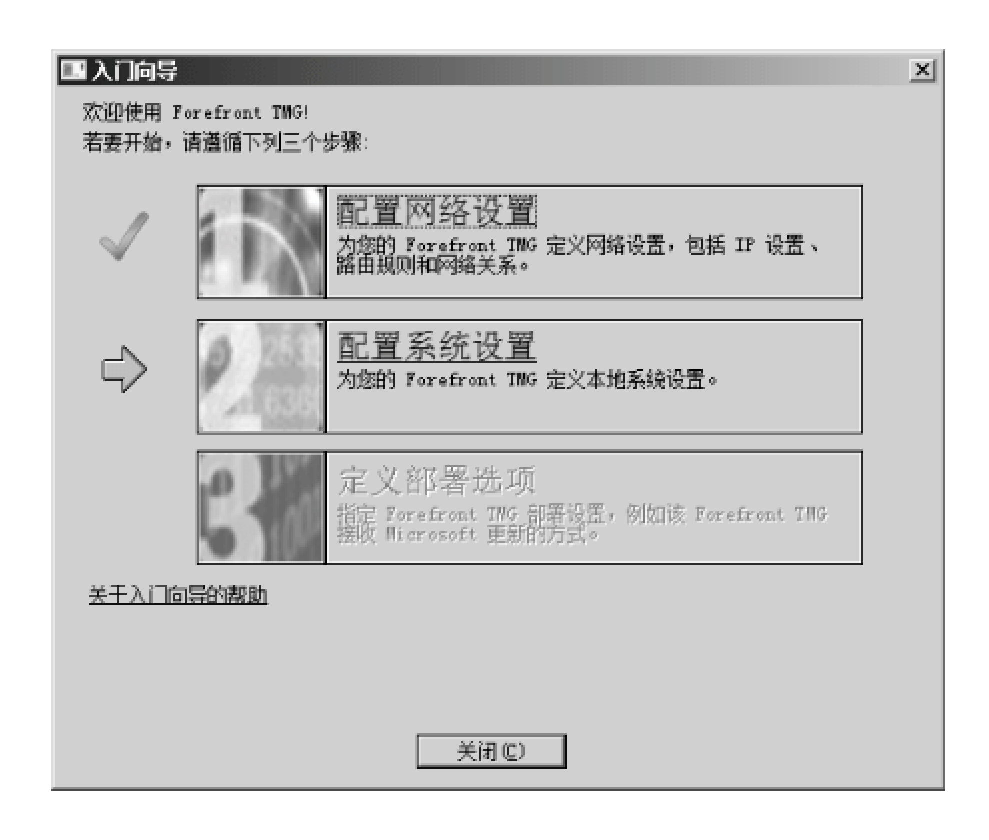


图 9-16 配置系统设置



图 9-17 系统配置向导

9.3.3 定义部署选项

当"系统配置向导"运行完成以后,"定义部署选项"就会变为可用状态,如图 9-18 所示,用来配置 Forefront TMG 的部署设置。

(1) 单击"定义部署选项"链接,启动"入门-部署向导"。连续单击"下一步"按钮,在如图 9-19 所示的"Microsoft Update 设置"对话框中,选中"使用 Microsoft Update 服务检查更新(推荐)"单选按钮。

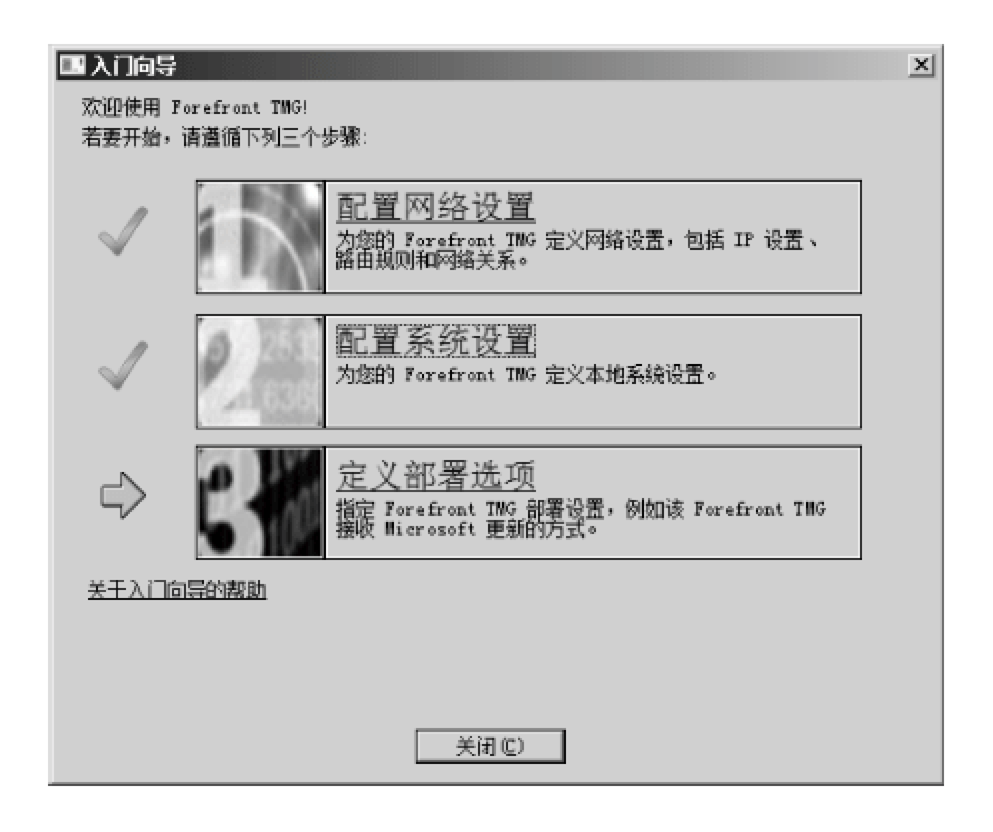


图 9-18 定义部署选项



图 9-19 "Microsoft Update 设置"对话框

(2) 在"定义更新设置"对话框中,选择恶意软件的检查方式和自动更新操作的轮询频率,如图 9-20 所示。

(3) 连接单击"下一步"按钮,完成部署向导,如图 9-21 所示。单击"完成"按钮返回"入门向导"对话框。

9.3.4 实现 Internet 共享

Forefront TMG 的"入门向导"还提供了"Web 访问策略向导"功能,通过该向导即可创建 Internet 连接共享策略,供内部网络的用户通过 Forefront TMG 访问 Internet 上的 Web 网站,而不必再手动创建专门的策略。



图 9-20 “定义更新设置”对话框



图 9-21 完成部署向导

（1）当配置网络设置、配置系统设置和定义部署选项全部配置完成以后，返回“入门向导”对话框，会发现多出了一个“运行 Web 访问向导”复选框，如图 9-22 所示。选中该项用来配置 Web 访问策略。

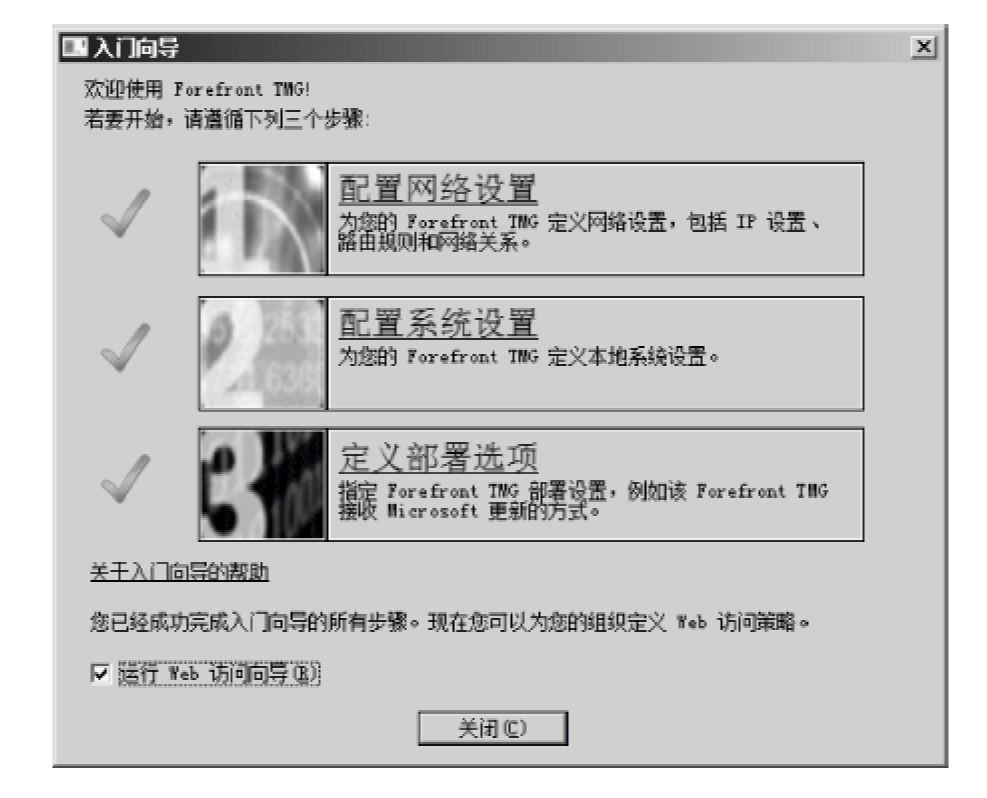


图 9-22 “入门向导”对话框

（2）单击“关闭”按钮，即可启动“Web 访问策略向导”。单击“下一步”按钮，显示“Web 保护”对话框，选中“是，启用恶意软件检查功能”单选按钮，如图 9-23 所示。

（3）单击“下一步”按钮，显示如图 9-24 所示的“Web 访问策略类型”对话框，可以选择以下选项。

① 为我的组织中的所有客户端创建简单的 Web 访问策略：如果选择该项，可创建允许内部网络的所有客户端计算机访问 Internet 的策略，这里选择该项。

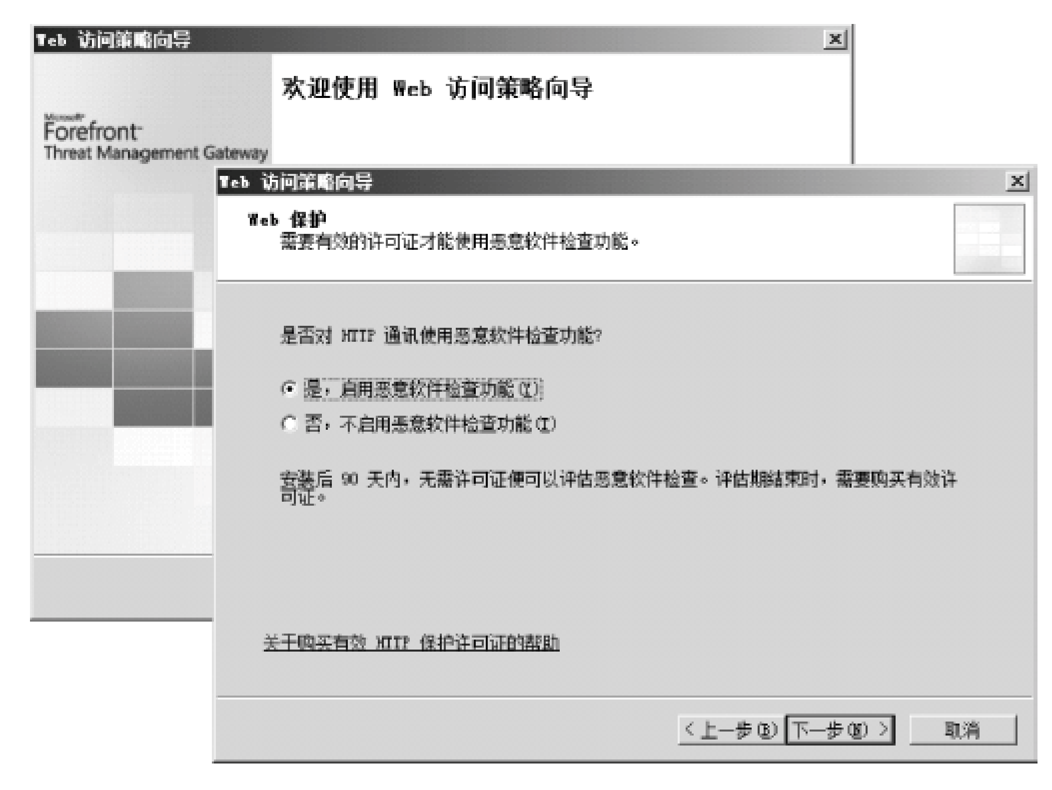


图 9-23 “Web 保护”对话框

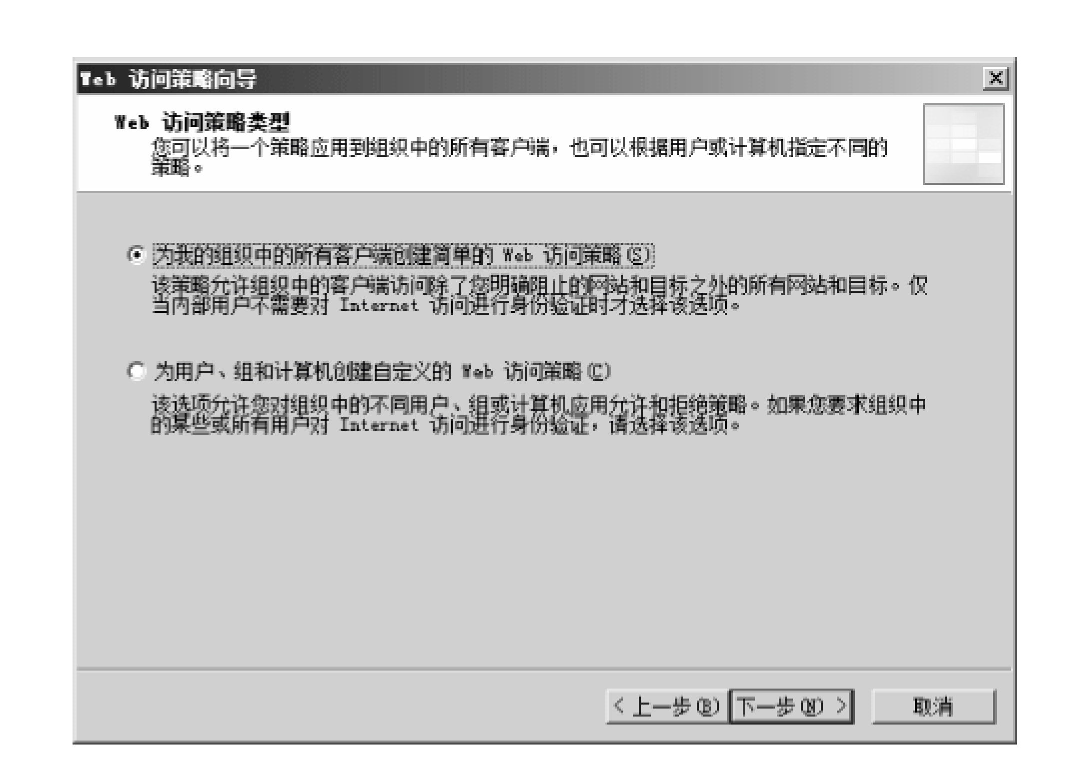


图 9-24 “Web 访问策略类型”对话框

② 为用户、组和计算机创建自定义的 Web 访问策略：如果选择该项，则可创建一个策略，允许或者拒绝内部网络中的用户或者计算机访问 Internet。用户通过 Forefront TMG 访问 Internet 时，需要进行身份验证。

(4) 单击“下一步”按钮，显示“受限制的 Web 目标”对话框，用来拒绝内部网络访问的 Web。单击“添加”按钮，显示“添加目标”对话框，可以添加欲限制访问的 URL 集、域名集、地址范围和网络，如图 9-25 所示。



图 9-25　“受限制的 Web 目标”对话框

例如，要禁止内网用户访问某些不良的 Web 站点，可单击“新建”菜单中的“新建 URL 集”选项，显示如图 9-26 所示的“新建 URL 集规则元素”对话框。在“名称”文本框中为该 URL 集输入一个名称，单击“添加”按钮，添加欲禁止访问的 Web 网址即可。

单击“确定”按钮返回“添加目标”对话框。展开“URL 集”，选择刚刚创建的 URL 集，单击“添加”按钮，即可添加到“受限制的 Web 目标”对话框。

(5) 单击“下一步”按钮，显示如图 9-27 所示的“受限制的目标例外”对话框。有时，限制访问的 Web 目标又需要被内网的某些用户访问，可单击“添加”按钮添加允许访问的用户。也可单击“新建”按钮，运行“新建用户集向导”来创建允许访问受限制目标的用户集。

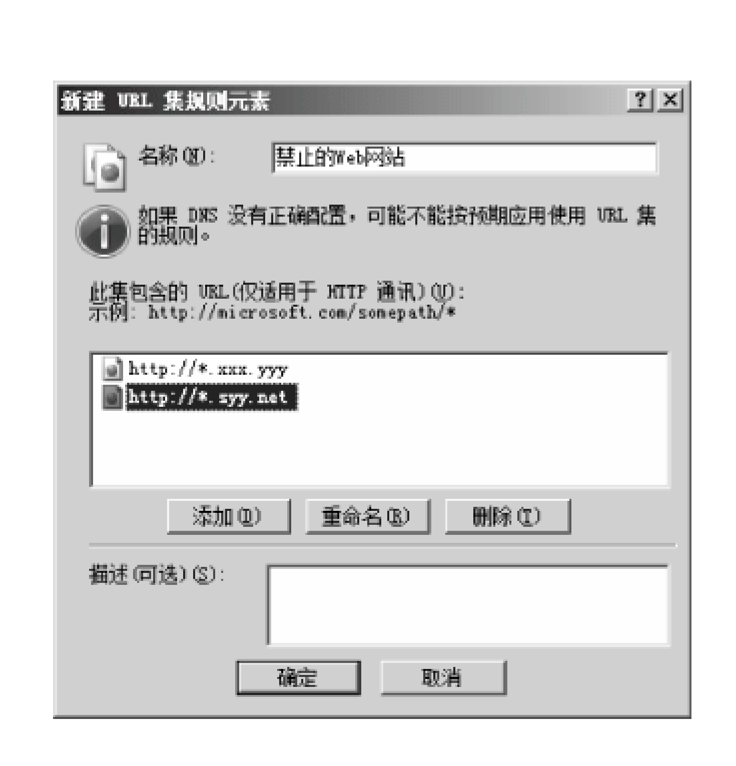


图 9-26　“新建 URL 集规则元素”对话框

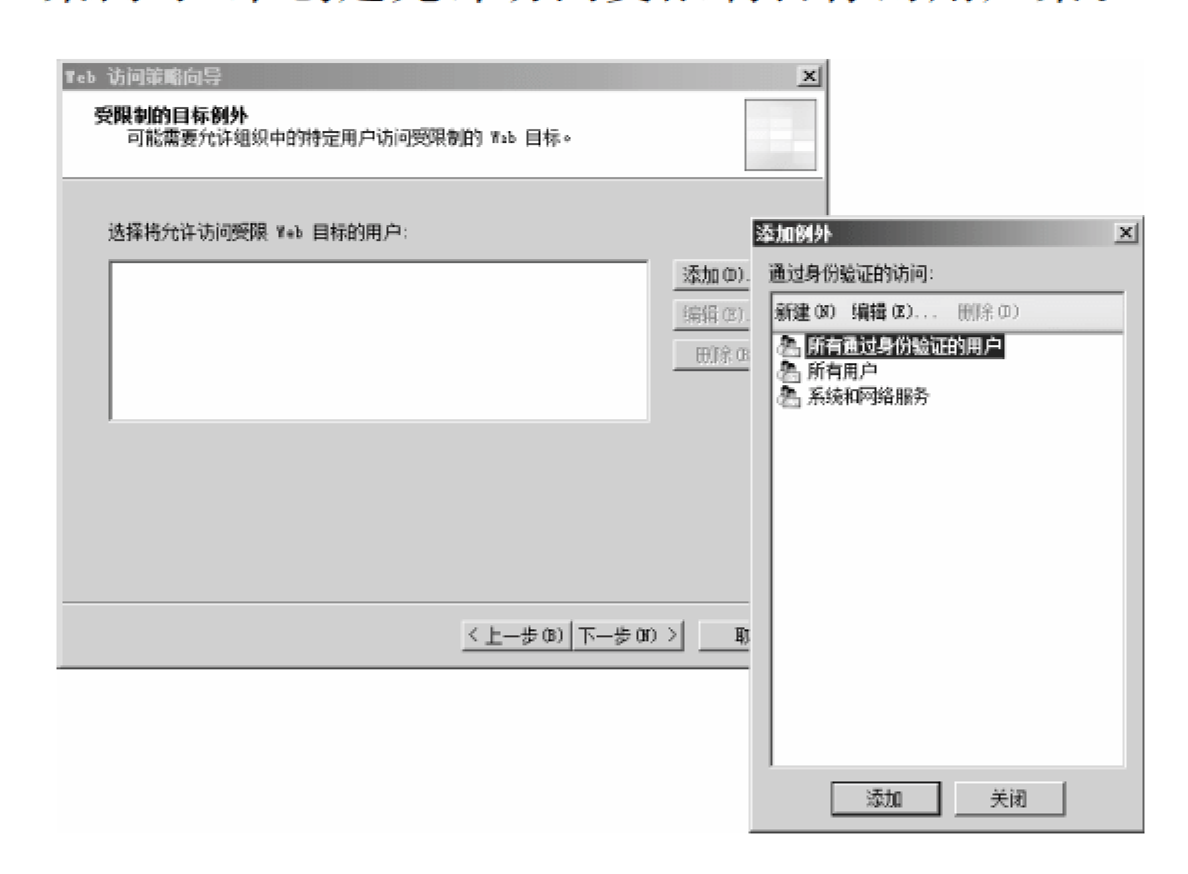


图 9-27　“受限制的目标例外”对话框

(6) 单击“下一步”按钮,显示如图 9-28 所示的“恶意软件检查设置”对话框,可选择是否检查从 Internet 请求的 Web 内容,以检查是否含有恶意软件。

(7) 单击“下一步”按钮,显示如图 9-29 所示的“Web 缓存配置”对话框,用来设置 Web 缓存,以提高内部网络访问 Web 网站的速度,并减少 Internet 带宽的消耗。

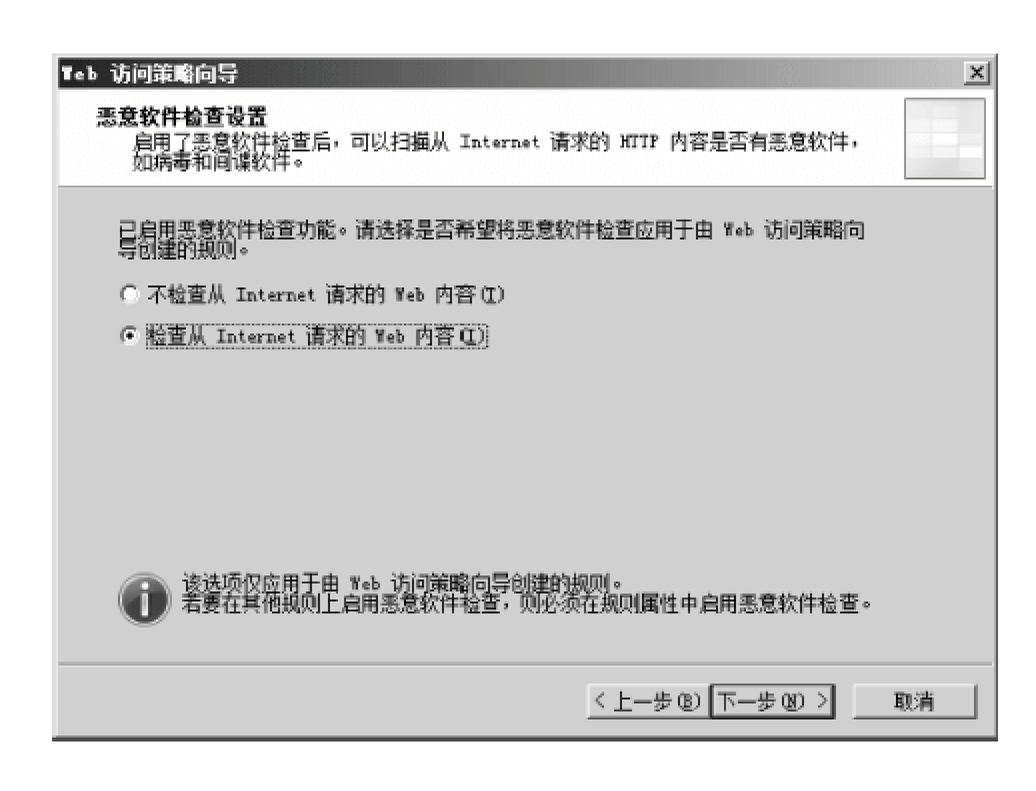


图 9-28 “恶意软件检查设置”对话框

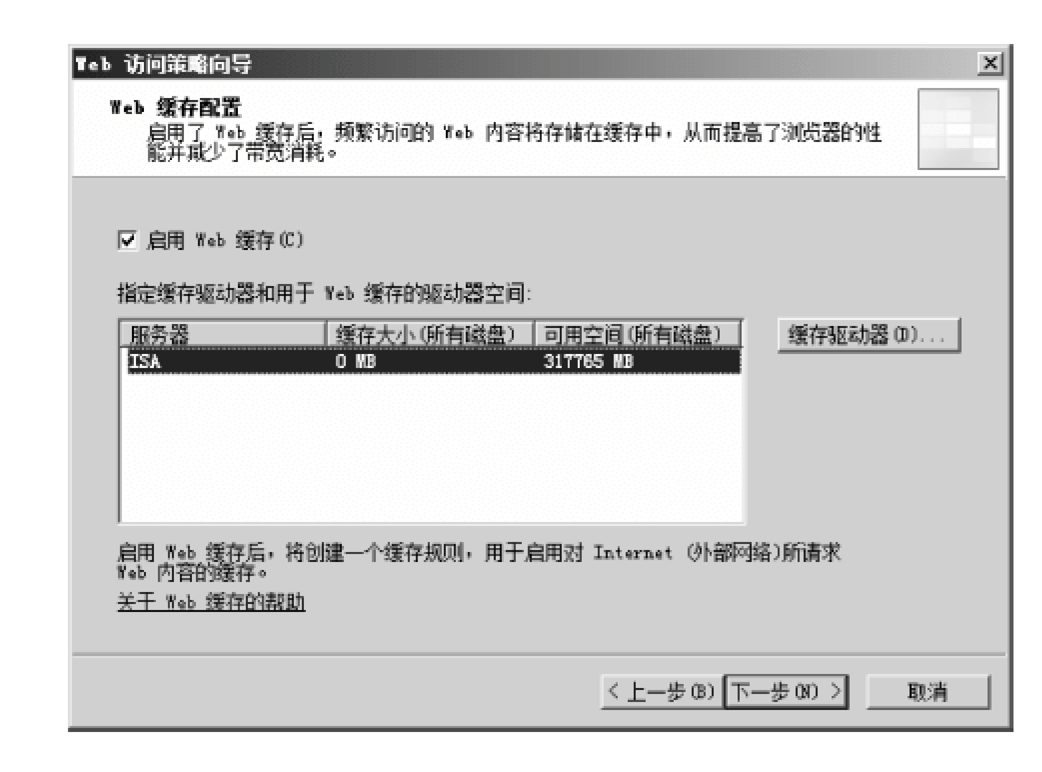


图 9-29 “Web 缓存配置”对话框

(8) 单击“缓存驱动器”按钮,显示如图 9-30 所示的“定义缓存驱动器”对话框。选择要设置缓存的驱动器,在“最大缓存大小”文本框中输入欲设置的缓存大小(以 MB 为单位),单击“设置”按钮即可。例如,这里设置 E 盘为缓存驱动器,缓存大小为 10000MB。单击“确定”按钮保存并返回。

提示: 为了使内网计算机访问 Internet 的速度更快,缓存自然是越大越好。当然,也要留出足够的空间用于保存其他数据。

(9) 单击“下一步”按钮,显示如图 9-31 所示的“正在完成 Web 访问策略向导”对话框,Web 访问策略向导完成。单击“完成”按钮,返回 Forefront TMG 控制台。

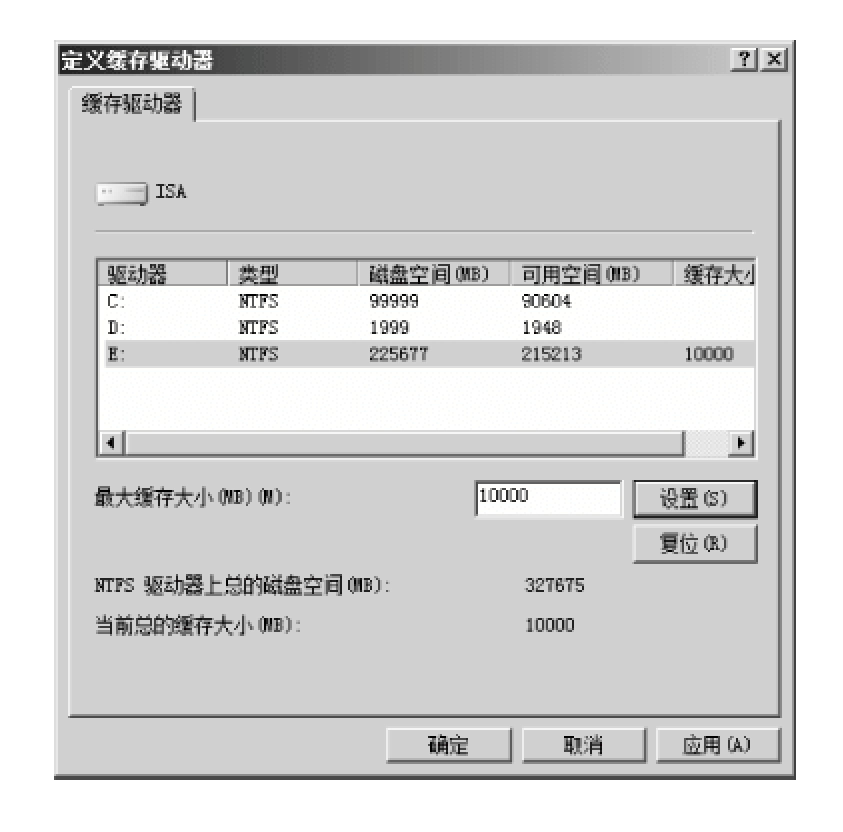


图 9-30 “定义缓存驱动器”对话框

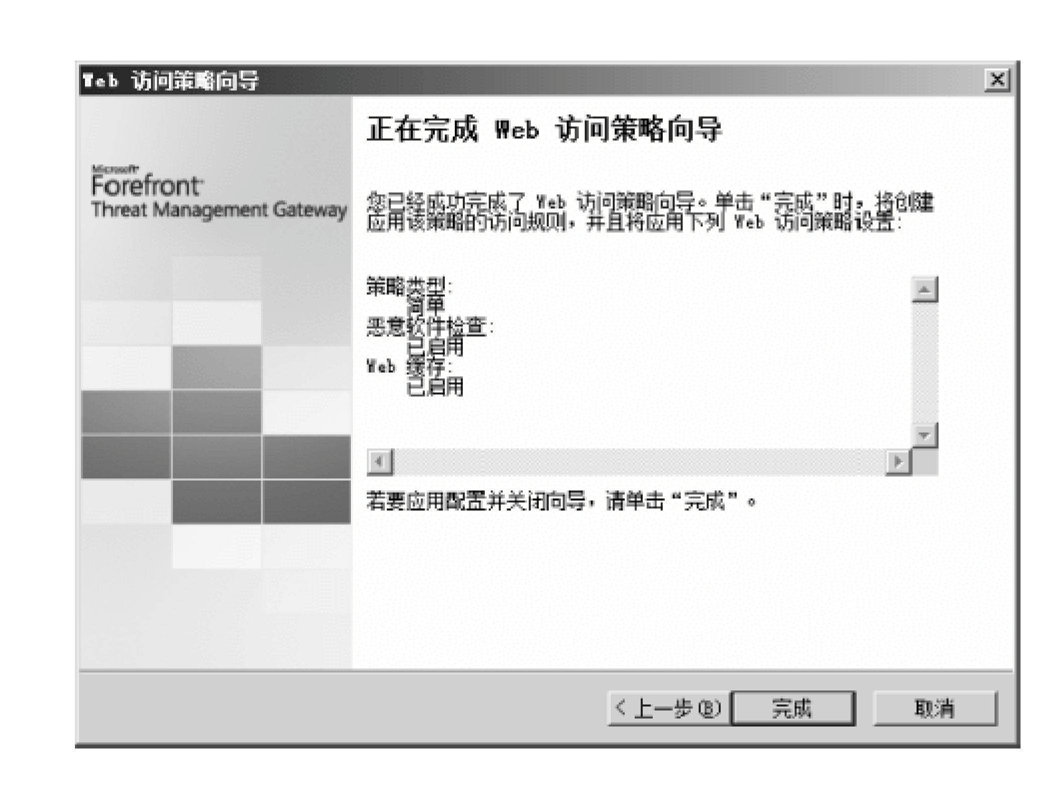


图 9-31 “正在完成 Web 访问策略向导”对话框

至此,Web 访问策略配置完成。如果当前服务器仅仅用来充当代理服务器功能,那么,不需进行其他设置,即可使局域网中的计算机连接 Internet 了。

9.3.5 配置 Web 访问策略

在 Forefront TMG 控制台中单击“Web 访问策略”选项,用来设置 Web 访问策略,如

图 9-32 所示。其中，“Web 访问限制”策略的操作方式为“拒绝”，用来设置阻止访问的行为；而“Web 访问默认规则”策略的操作方式为“允许”，用来设置允许访问的行为。不过，新创建的策略尚未生效，因此，提示需要单击“应用”来保存更改并更新配置。

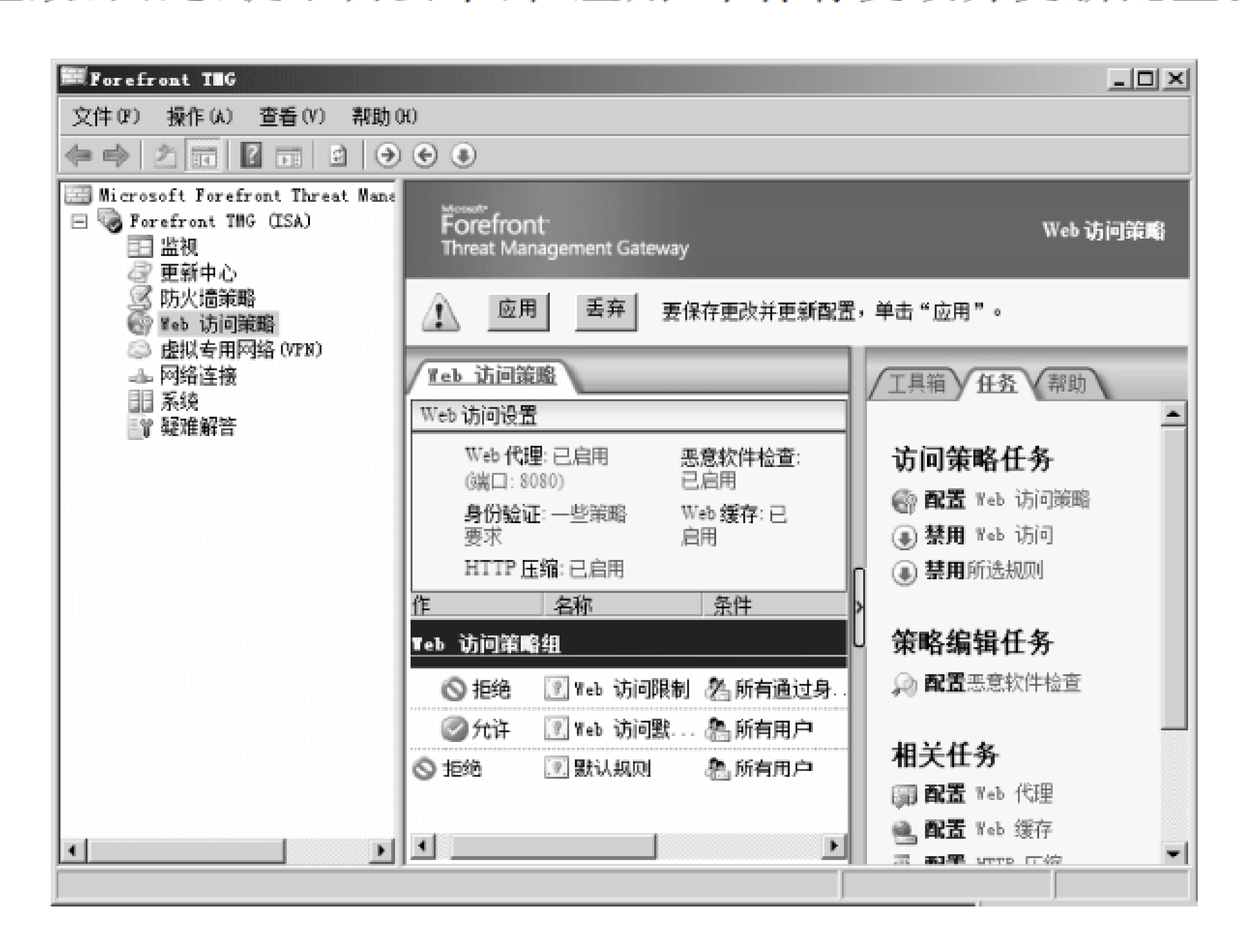


图 9-32 Web 访问策略

提示：单击“任务”选项卡中的“配置 Web 访问策略”链接，可以重新启动“Web 访问策略向导”进行配置，不过，原来手动配置的 Web 访问策略将会被丢弃。

（1）单击“应用”按钮，显示如图 9-33 所示的“Forefront TMG 警告”对话框。选中“保存更改，并重启动服务”单选按钮，单击“确定”按钮，即可开始应用更改。

（2）单击“确定”按钮，显示如图 9-34 所示的“正在保存配置更改”对话框，所做的更改应用完成。单击“确定”按钮关闭即可。



图 9-33 “Forefront TMG 警告”对话框

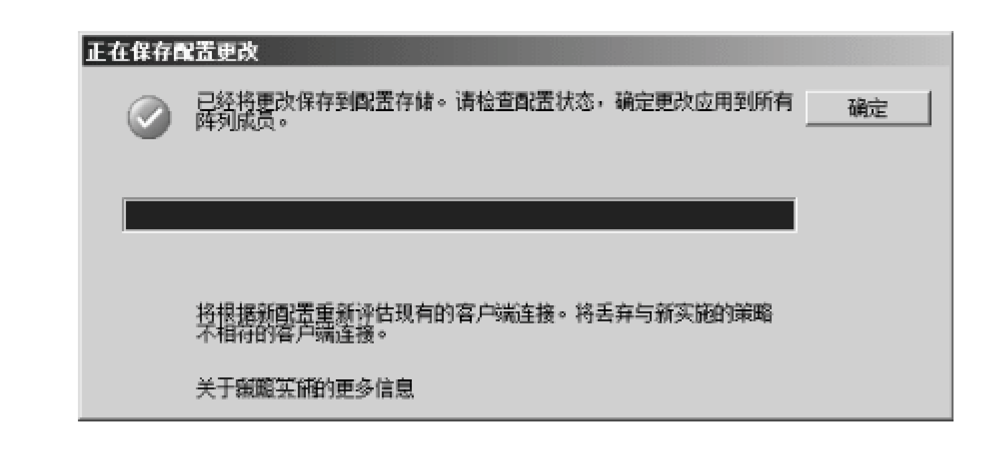


图 9-34 “正在保存配置更改”对话框

（3）如果需要重新配置 Web 访问策略，可选择相应的策略，例如“Web 访问限制”，右击并选择快捷菜单中的“属性”选项，显示如图 9-35 所示的“Web 访问限制 属性”对话框。如果要禁用该策略，可取消选中“启用”复选框。

（4）切换到“协议”选项卡，可以设置当前策略所控制的协议，如图 9-36 所示。

（5）在“从”和“到”选项卡中，可以分别设置源和目标的通信，如图 9-37 所示。例如，Internet 上有很多违法或不良网站，为了防止内网用户访问，就可以在“到”选项卡中通过添加 IP 地址、域名或 URL 的方式将其阻止。其操作步骤和运行“Web 访问策略向导”时相同。



图 9-35 “Web 访问限制 属性”对话框



图 9-36 “协议”选项卡

(6) 在“用户”选项卡中,可以设置此策略应用于哪些用户,如图 9-38 所示。

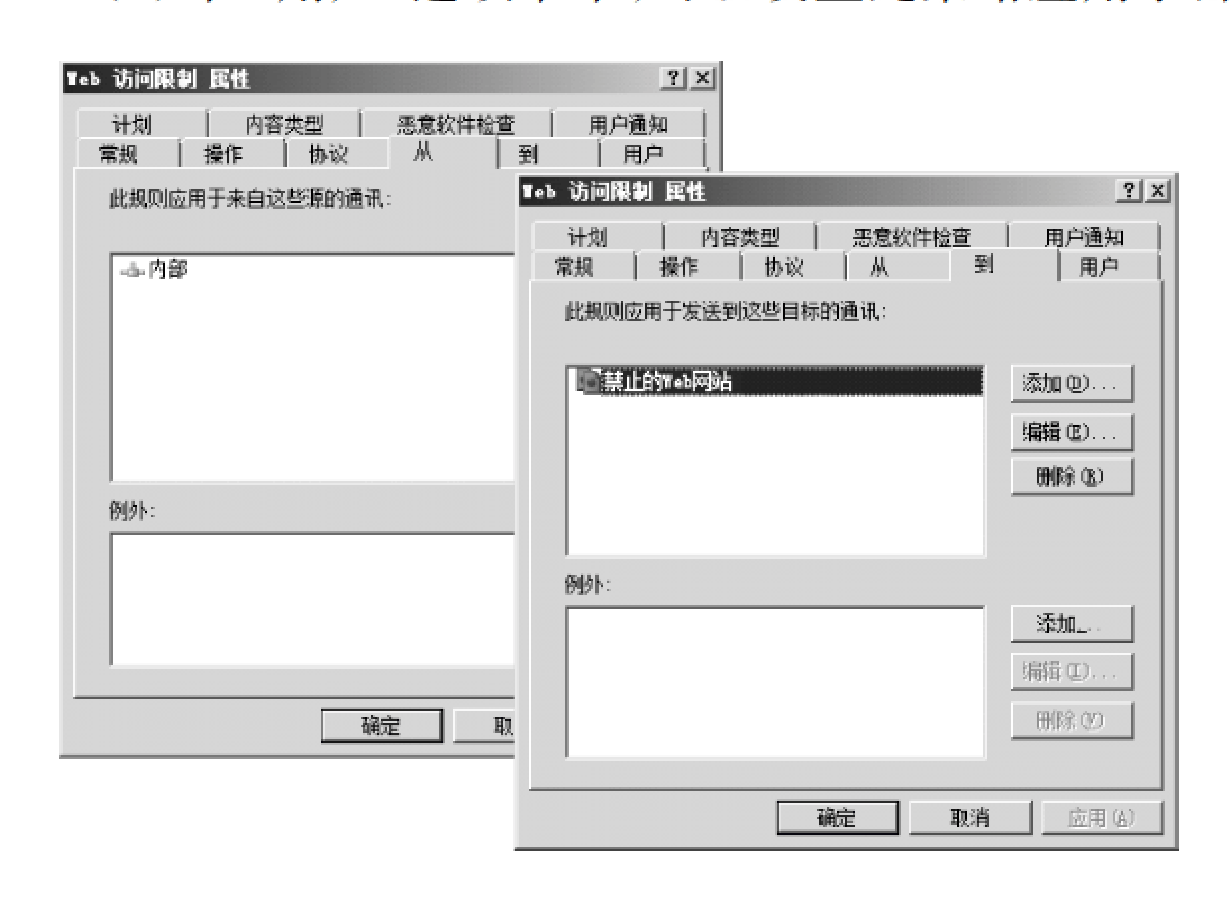


图 9-37 “从”和“到”选项卡

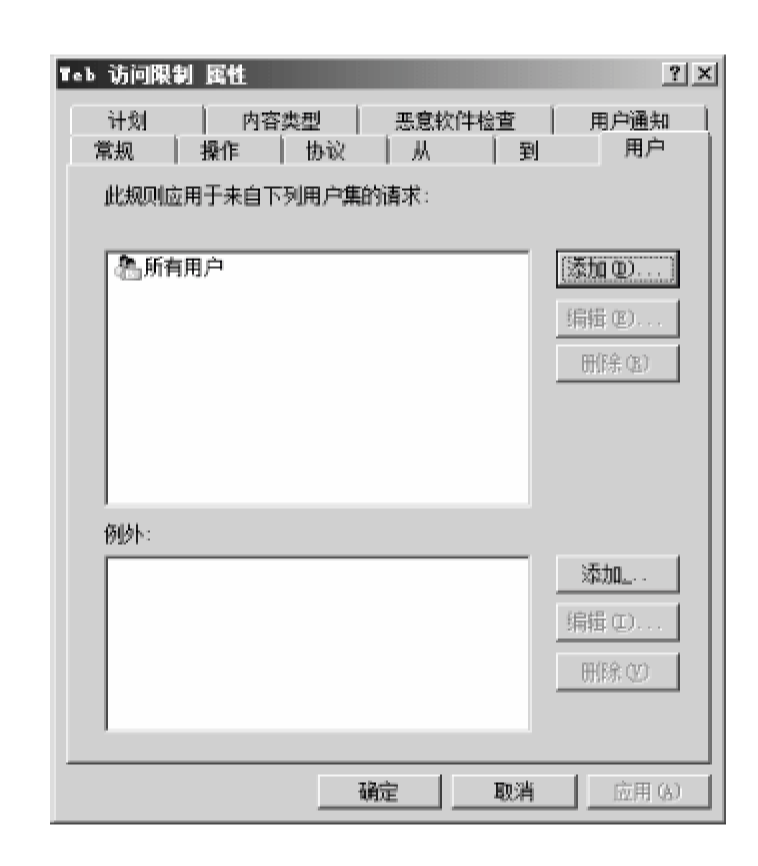


图 9-38 “用户”选项卡

(7) 在“计划”选项卡中,可以设置当前策略的执行时间,如图 9-39 所示。例如,要允许内网用户只能在工作时间上网,就可以将时间范围选择为从星期一的 8 点至星期五的 5 点。

(8) 选择如图 9-40 所示的“内容类型”选项卡,可以设置该策略可用于哪些类型,默认应用于所有内容类型。

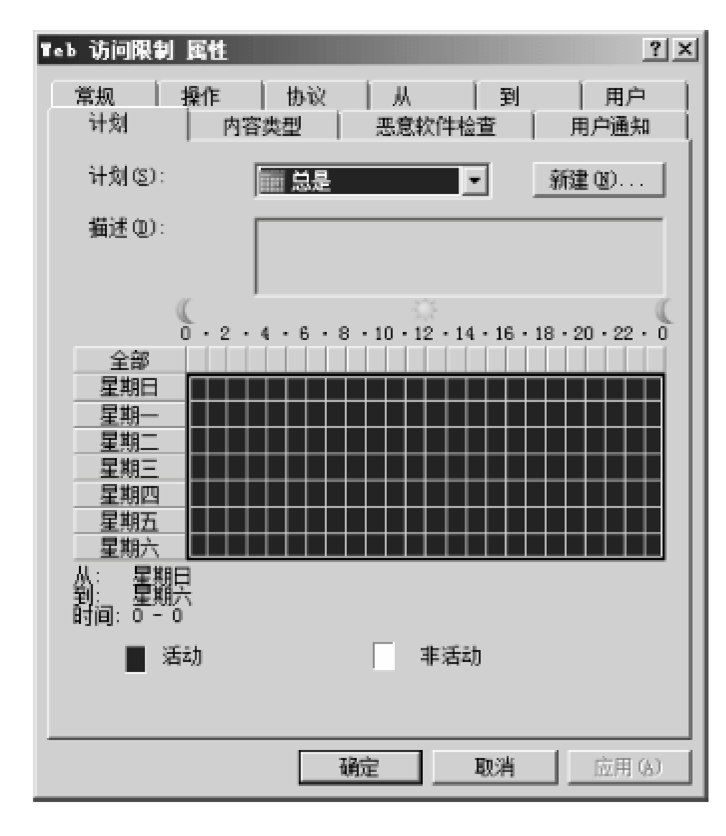


图 9-39 “计划”选项卡

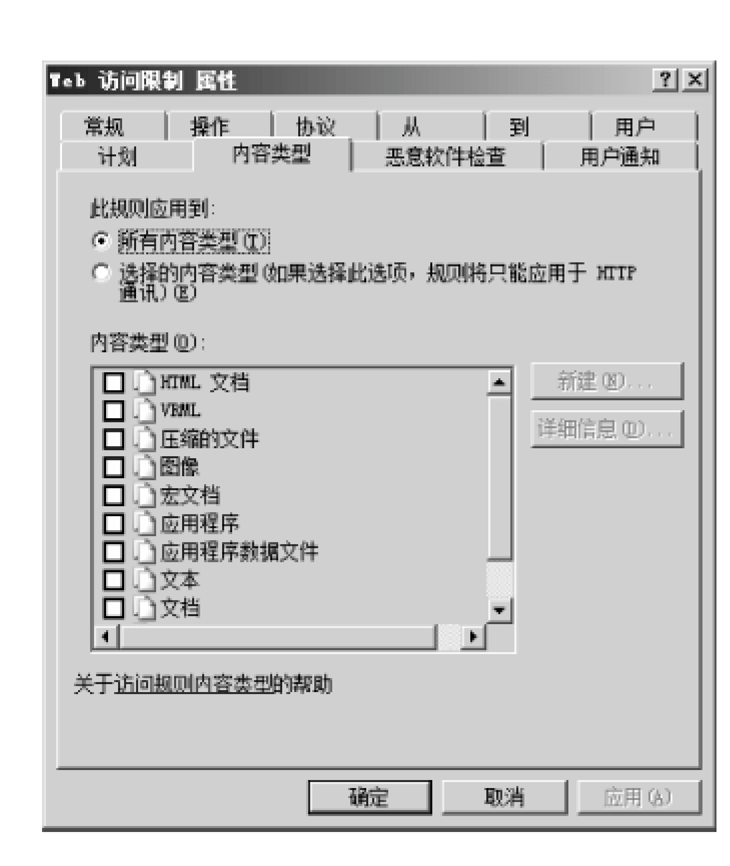


图 9-40 “内容类型”选项卡

9.3.6 知识链接：Forefront TMG 中的网络

在 Forefront TMG 网络中，分为“内部”、“本地主机”、“外部”、“VPN 客户端”和“被隔离的 VPN 客户端”共 5 部分。这些网络的功能和意义分别如下。

（1）内部：代表内部局域网。TMG 防火墙将内部网络代表受信任和受保护的网络，默认允许本地主机访问内部网络上的资源，但拒绝其他任何网络访问内部网络，必须创建规则来允许到内部网络的访问。

（2）本地主机：代表 TMG 服务器本身。与 TMG 防火墙之间的所有通信都被认为是和本地主机网络之间的通信。

（3）外部：指连接到 Internet 的网络，通常被视为不受信任的网络。

（4）VPN 客户端：代表通过 VPN 连接到 ISA 服务器的客户端计算机，由 TMG 防火墙动态生成。

（5）被隔离的 VPN 客户端：包含尚未解除隔离的 VPN 客户端的地址，由 TMG 防火墙动态生成。

除了上述的 5 部分网络，如果 Forefront TMG 被配置成“3 向外围网络”，还包括“外围”网络。“外围”网络也称为 DMZ(Demilitarized Zone)。DMZ 通常用于放置公共信息，用户、潜在用户和外部访问者都可以直接访问 DMZ 区域，而不必通过内网。目前，许多硬件防火墙都集成了 DMZ 接口。Forefront TMG 也可以在安装 3 块网卡（或者更多）的情况下，配置成“3 向外围网络”。

9.4 Internet 接入安全管理

TMG 功能强大，设置和使用十分方便。TMG 不仅将网络划分为内网和外网，还多了一个“本地主机”部分，从而进一步提高企业网络的安全性。通过“入门向导”的配置，已经创建了基本的 Web 访问策略。除此之外，管理员还可以根据需要配置相关的防火墙策略，例如限制客户端访问 Internet 时间、限制下载文件的类型等。默认情况下，未经管理员明确允许的访问 Internet 的行为，都会被 TMG 服务器阻止。

9.4.1 限制部分用户访问 Internet 的时间

使用 TMG 的访问规则，可以控制指定的用户在指定的时间是否能够访问互联网。在部署访问规则前，需要在 Active Directory 中创建一个控制用户访问的安全组，将需要控制的用户添加到该组中。使用 TMG 管理控制台创建时间控制区域，然后通过规则设置访问的操作。

（1）打开 Forefront TMG 管理控制台，右击“防火墙策略”并选择快捷菜单中的“新建”→“访问规则”选项，显示如图 9-41 所示的“欢迎使用新建访问规则向导”对话框。在“访问规则名称”文本框中输入规则名称，例如“限制职工访问 Internet 的时间”等。

（2）单击“下一步”按钮，显示如图 9-42 所示的“规则操作”对话框，选中“拒绝”单选按钮。



图 9-41 “欢迎使用新建访问规则向导”对话框

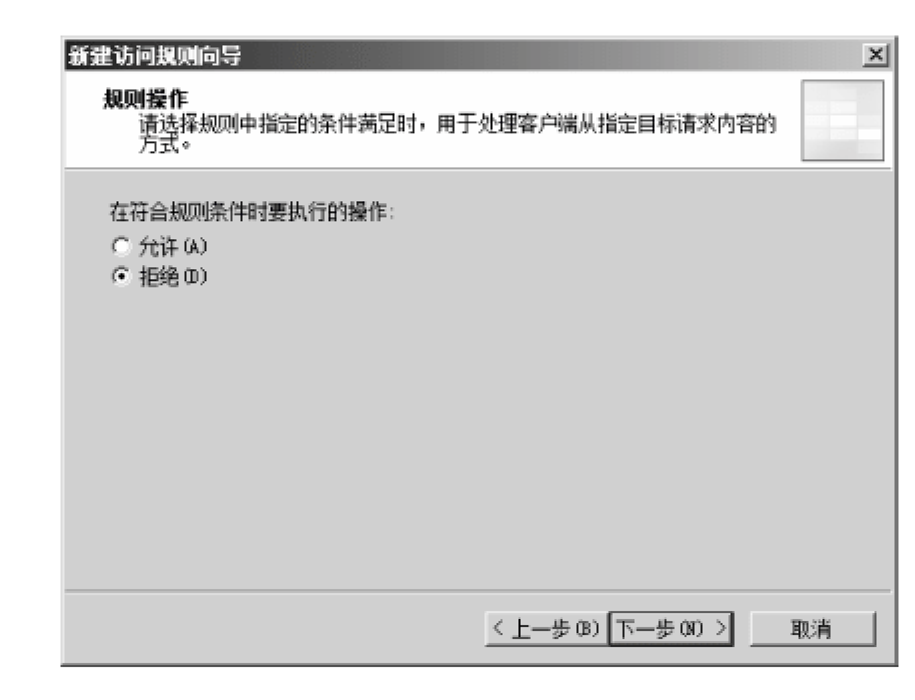


图 9-42 “规则操作”对话框

(3) 单击“下一步”按钮，显示如图 9-43 所示的“协议”对话框，在“此规则应用到”下拉列表框中选择“所选的协议”选项，并单击“添加”按钮，添加客户端用户使用的网络协议即可。

(4) 单击“下一步”按钮，显示如图 9-44 所示的“访问规则源”对话框，单击“添加”按钮，在“添加网络实体”对话框中选择“网络”→“内部”选项，单击“添加”按钮，将其添加到“访问规则源”列表中。




图 9-43 “协议”对话框



图 9-44 “访问规则源”对话框

(5) 单击“下一步”按钮，显示如图 9-45 所示的“访问规则目标”对话框，使用相同的方法，将访问规则的目标指定为“外部”即可。

(6) 单击“下一步”按钮，显示如图 9-46 所示的“用户集”对话框，删除默认的“所有用户”，单击“添加”按钮，显示“用户集”对话框，目前“用户集”中并没有所需的“职工”用户集，需要手动创建。单击“新建”按钮，启动“新建用户集向导”，在“用户集名称”文本框中，输入“职工”。

(7) 单击“下一步”按钮，显示如图 9-47 所示的“用户”对话框，单击“添加”按钮，显示“选择用户或组”对话框，将查找位置更改为当前域，输入需要添加的用户组或用户账户名称即可。




图 9-45 “访问规则目标”对话框

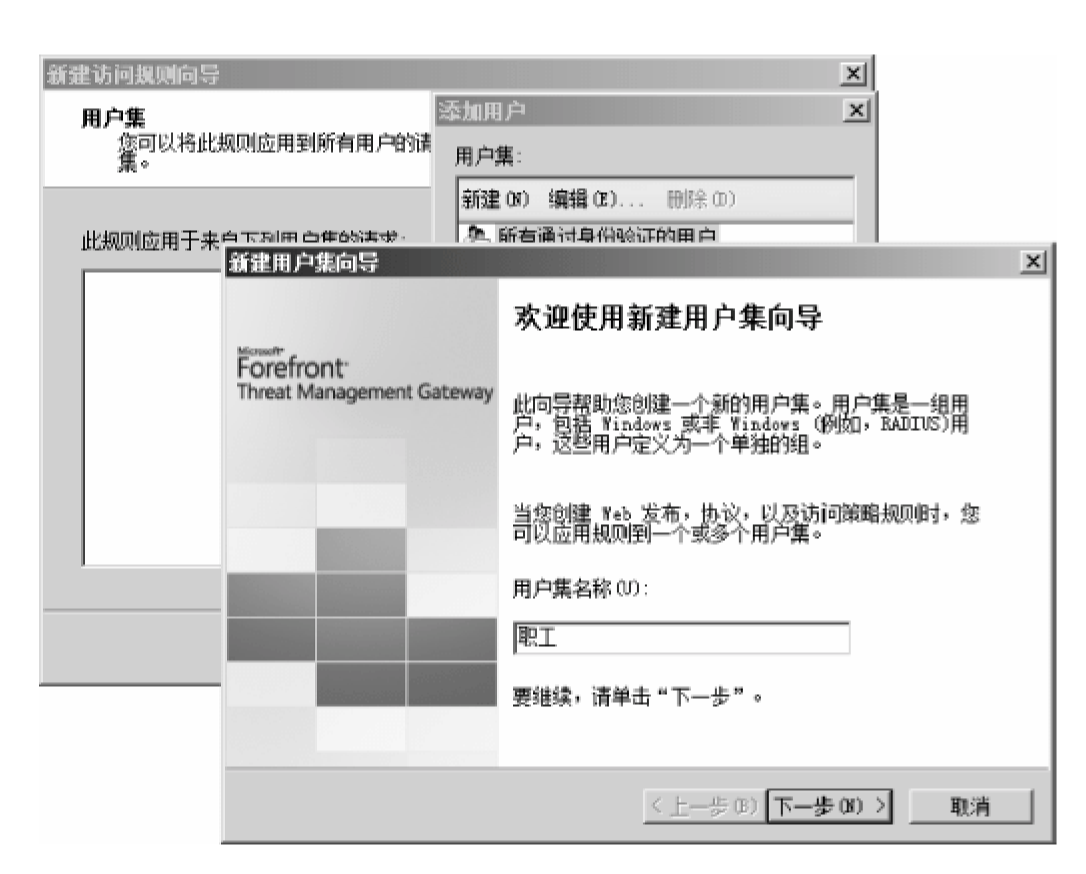


图 9-46 “用户集”对话框

（8）连续单击“确定”按钮，完成“职工”用户集的创建并返回到“新建访问规则向导”，将“职工”用户集添加到列表中，如图 9-48 所示。

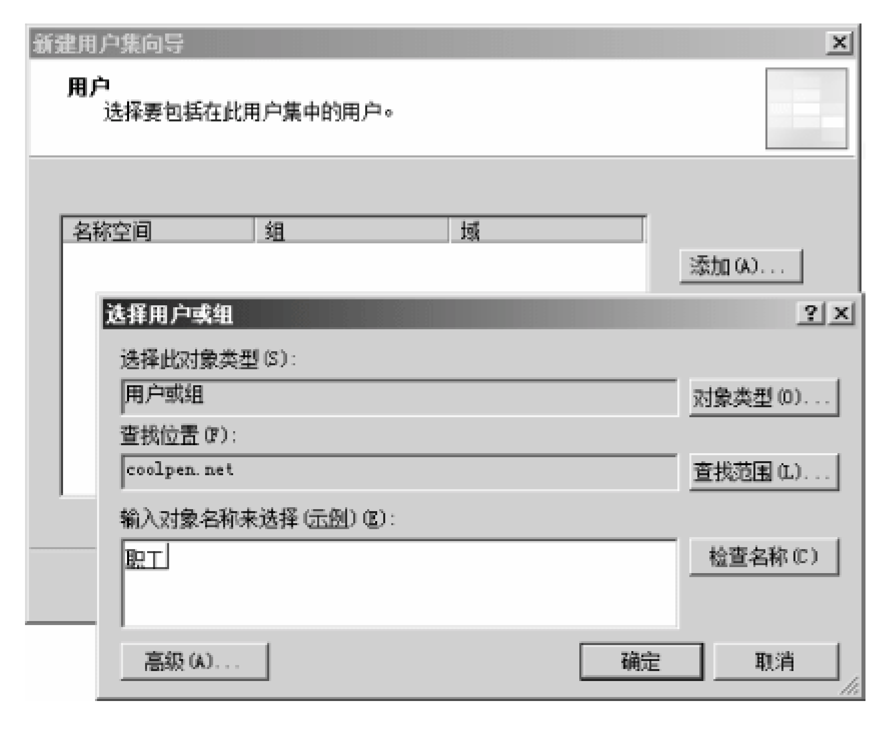


图 9-47 “用户”对话框

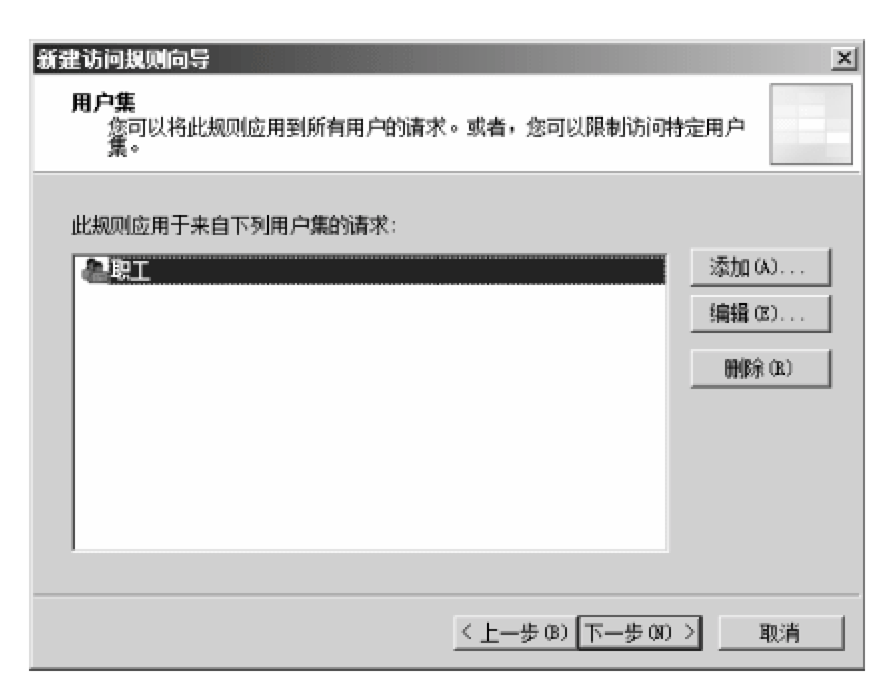


图 9-48 成功添加“职工”用户集

（9）单击“下一步”按钮，显示如图 9-49 所示的“正在完成新建 访问规则 向导”对话框。继续单击“完成”按钮，即可成功创建访问规则。

（10）在 Forefront TMG 管理控制台窗口中，右击创建的“限制职工访问 Internet 的时间”访问规则，选择快捷菜单中的“属性”选项，显示如图 9-50 所示的“限制职工访问 Internet

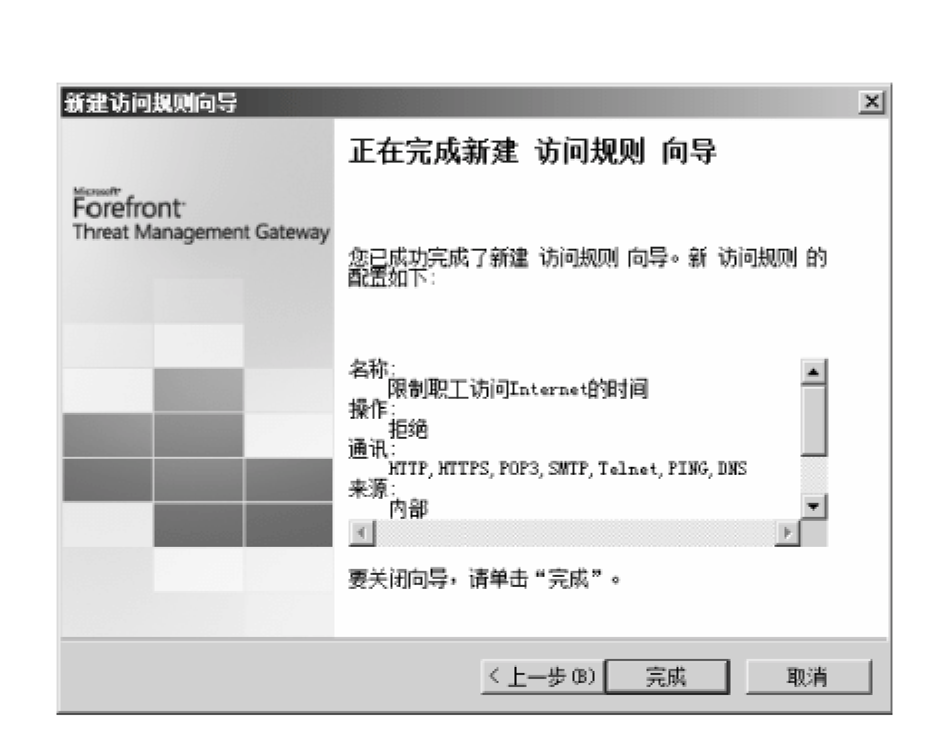


图 9-49 “正在完成新建 访问规则 向导”对话框

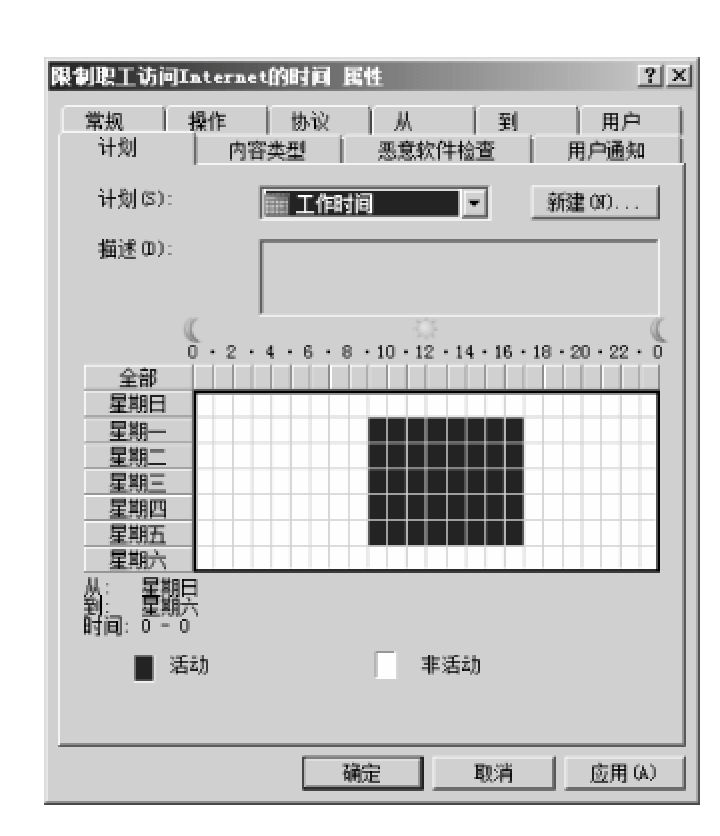


图 9-50 “限制职工访问 Internet 的时间 属性”对话框

的时间 属性”对话框，切换到“计划”选项卡，在“计划”下拉列表框中选择“工作时间”选项，如果现有计划内容与实际需求不符，则可以单击“新建”按钮，添加新的计划。

(11) 单击“确定”按钮，返回 Forefront TMG 管理控制台，应用该访问规则即可成功限制职工用户在工作时间访问 Internet。

9.4.2 禁止用户下载危险内容

使用 HTTP 过滤器，可以根据文件的扩展名进行限制。例如，禁止当前网页运行某些控件；禁止可执行文件下载，以防止木马或病毒自动入侵；禁止网页中的 BT 种子连接等，都可以通过阻止文件扩展名来实现。

(1) 在 Forefront TMG 窗口中，创建“允许”用户下载文件的访问规则，也可以直接编辑默认创建的“Web 访问默认规则”，确保规则中包含用户可能使用的下载协议即可，例如 HTTP、FTP 等。右击希望编辑的访问规则，选择快捷菜单中的“配置 HTTP”选项，显示如图 9-51 所示的“为规则配置 HTTP 策略”对话框。切换到“扩展名”选项卡，在“指定对文件扩展名要执行的操作”下拉列表框中选择“阻止指定的扩展名(允许所有其他扩展名)”选项。



图 9-51 “为规则配置 HTTP 策略”对话框

(2) 单击“添加”按钮，显示如图 9-52 所示的“扩展名”对话框。在“扩展名”文本框中输入要阻止的扩展名，在“描述(可选)”文本框中输入说明信息。

(3) 单击“确定”按钮，扩展名类型添加成功。按照同样操作步骤，可以添加多种扩展名，如图 9-53 所示。

(4) 单击“确定”按钮，保存设置，并应用设置使其生效即可。

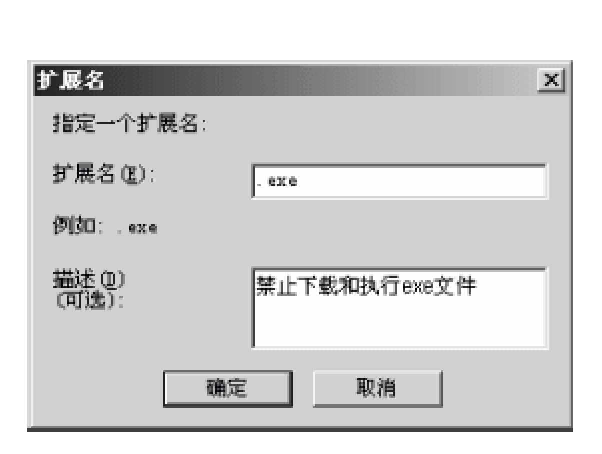


图 9-52 “扩展名”对话框

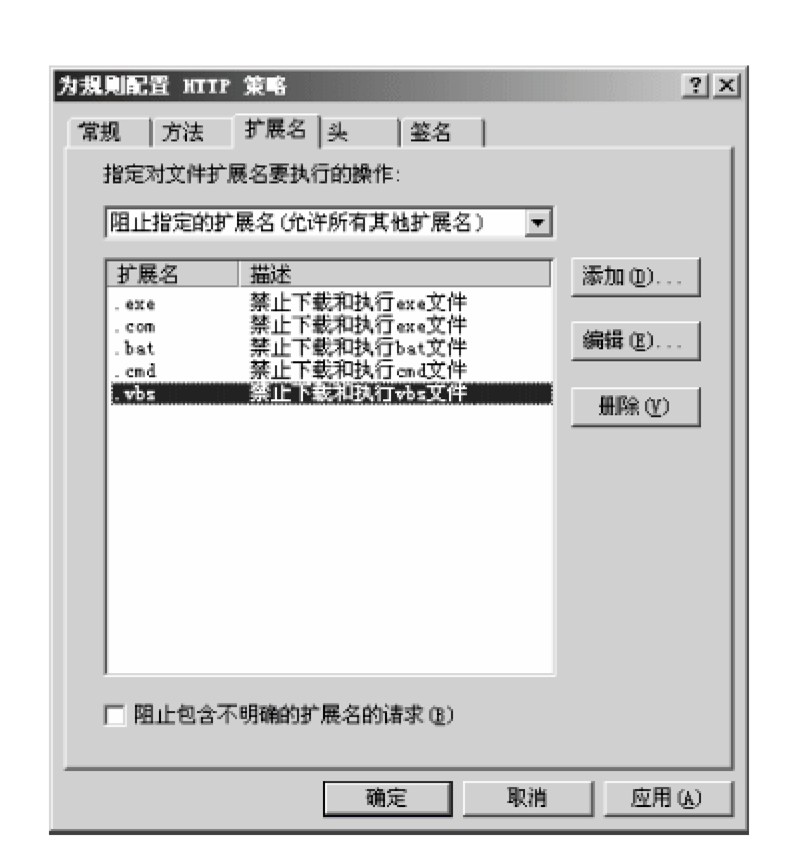


图 9-53 成功添加所有希望阻止的扩展名

9.4.3 禁用使用即时消息软件

在企业中，为了不影响用户的工作，往往禁止在上班时上网聊天。这可以在 Forefront TMG 中进行限制。Forefront TMG 默认提供了 AOL、ICQ、IRC、Net2Phone、MSN Messenger 等软件的协议，而对于一些国内即时通信软件却没有提供，如 QQ、UC 等，需要由用户手动添加。

1. 添加 QQ 和 UC 协议

QQ 使用 UDP 和 TCP 协议的 4000～4010 端口和 8000～8010 端口。而 UC 使用 UDP 协议，端口为 3001、3002。需要在 TMG 中添加 QQ 和 UC 的协议，准备创建禁用规则。

(1) 打开 TMG 的"防火墙策略"窗口，在右侧列表中选择"工具箱"选项卡，并选择"协议"选项组，如图 9-54 所示。



图 9-54 "协议"选项组

(2) 单击"新建"按钮，选择下拉菜单中的"协议"选项，运行"新建协议定义向导"。在"首要连接信息"对话框中，用来设置端口号和协议。单击"新建"按钮，显示如图 9-55 所示的"新建/编辑协议连接"对话框，设置如下选项。

① 协议类型：在下拉列表框中选择 UDP 选项。

② 方向：在下拉列表框中选择发送接收选项。

③ 端口范围：分别输入 4000 和 4010。

(3) 单击"确定"按钮添加。然后，再次单击"新建"按钮，添加端口范围为 8000～8010 的 UDP 协议。连续单击"下一步"按钮，在"辅助连接"对话框中选中"否"单选按钮。在"正在完成新建协议定义向导"对话框中，单击"完成"按钮即可，如图 9-56 所示。

(4) 再次运行"新建协议定义向导"，添加 UC 协议。UC 协议的"协议类型"为 UDP，"方向"为"发送接收"，"端口范围"为 3000～3002。

添加完成的 QQ 和 UC 协议将显示在"防火墙策略"的"用户定义"列表中，如图 9-57 所示。然后，即可创建防火墙策略，来限制这两种协议的通信。

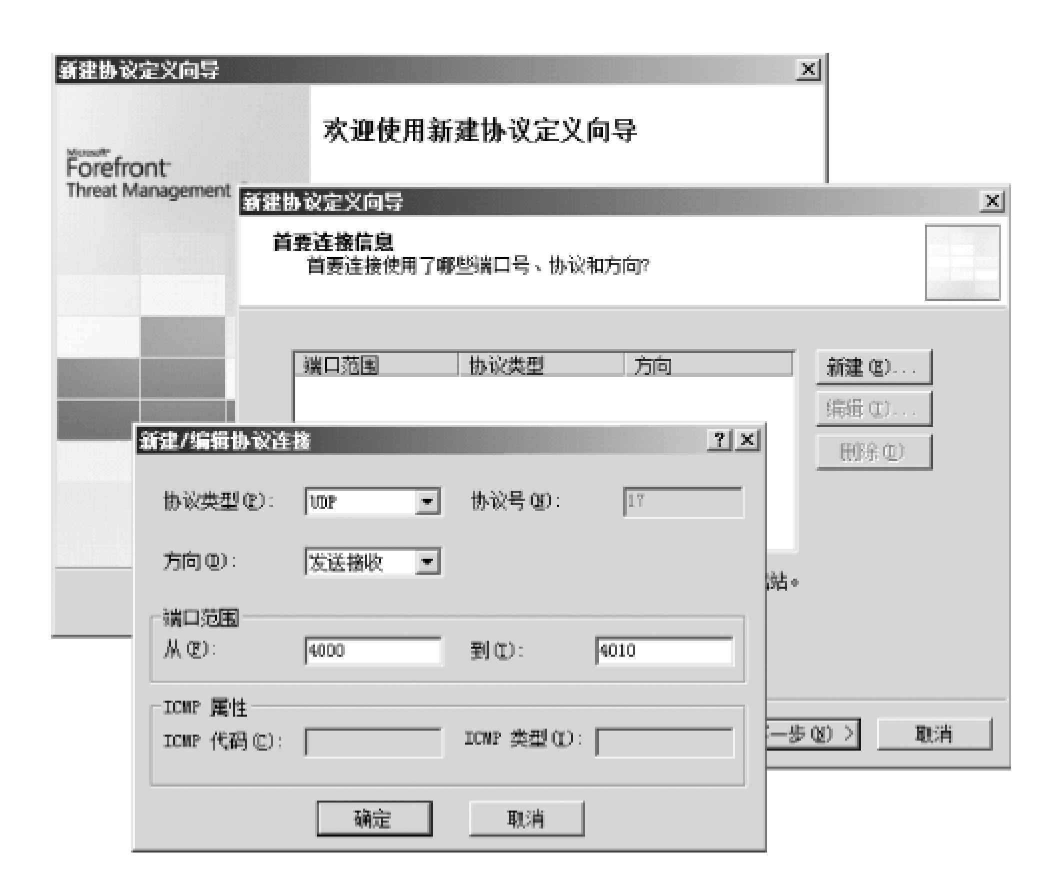



图 9-55 “新建编辑协议连接”对话框



图 9-56 “辅助连接”对话框



图 9-57 添加的 QQ 和 UC 协议

2. 添加防火墙规则

要限制内网用户使用 QQ、UC 等即时通信软件，就需要添加一条规则，拒绝所添加的 QQ 和 UC 协议的通信，从而使内网中的用户无法登录 QQ 和 UC。用户也可以在原有访问规则基础上进行适当编辑，添加相关网络协议即可。

(1) 在“防火墙策略”窗口中，运行“新建访问规则向导”。在“规则操作”对话框中选中“拒绝”单选按钮；在“协议”对话框中，单击“添加”按钮，添加“用户定义”中的 QQ 和 UC 协议，如图 9-58 所示。

(2) 连续单击“下一步”按钮，在“访问规则源”对话框中添加“内部”；在“访问规则目标”对话框中添加“外部”。规则创建完成以后，还可设置时间计划，设置为只在上班时间禁用 QQ 和 UC。右击该规则并选择快捷菜单中的“属性”选项，打开规则属性对话框。选择“计划”选项卡，在“计划”下拉列表框中选择“工作时间”选项即可，如图 9-59 所示。

(3) 依次单击“确定”按钮保存，并单击“应用”按钮使规则生效。

这样，在上班时间，用户就不能使用 QQ 和 UC 软件了。





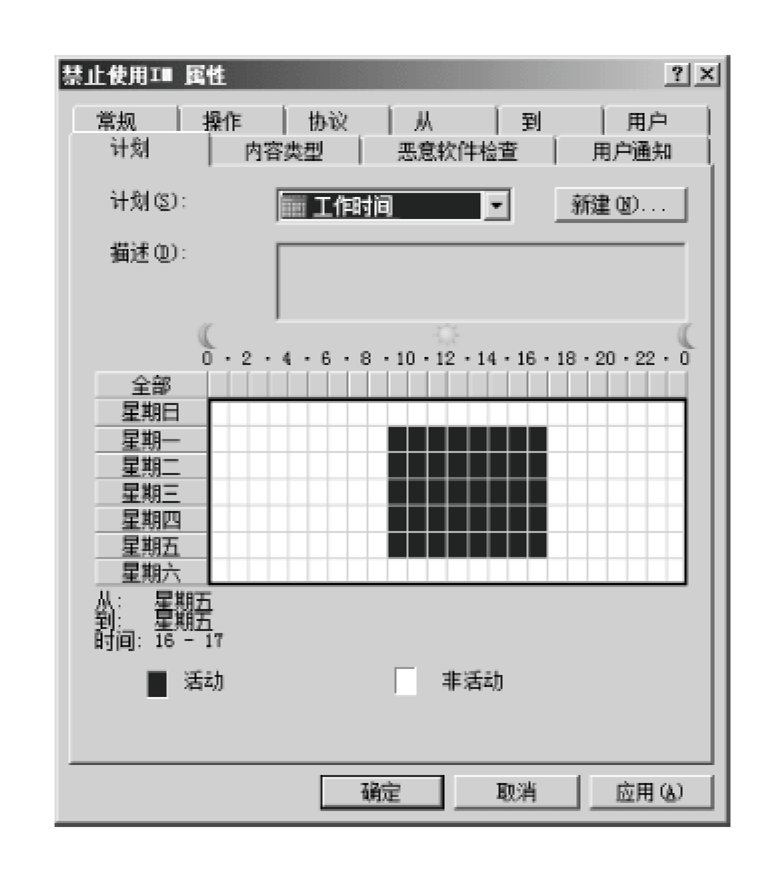


图 9-58 添加 QQ 和 UC 协议 图 9-59 "计划"选项卡

9.4.4 禁止用户观看流媒体

允许内部网络用户访问互联网,但是不允许在正常工作时间观看流媒体。观看流媒体时占用带宽比较高,如果 100Mbps 的 Internet 线路有几十个用户同时在观看流媒体,其他人访问互联网速度会明显变慢。在 TMG 中,创建一条新的规则"禁止观看流媒体",禁止访问流媒体服务器。目前的流媒体主要采用 MMS、MMS 服务器、RTSP、RTSP 服务器等协议。

(1) 在防火墙策略窗口中,启动"新建访问规则向导",创建一条新的防火墙策略。在"规则操作"对话框中选择"拒绝"选项。在"协议"对话框中,选择"此规则应用到"下拉列表框中的"所选的协议"选项。单击"添加"按钮,显示"添加协议"对话框,将"流媒体"中所有网络协议添加到列表中即可,如图 9-60 所示。



图 9-60 添加所有流媒体协议

(2) 在"访问规则源"对话框中添加"内部"选项。在"访问规则目标"对话框中添加"外部"选项。在"用户集"对话框中添加"所有用户"选项。单击"完成"按钮,完成访问规则的创建。

新规则创建完成以后,单击"应用"按钮使规则生效,用户就不能观看使用选择的流媒体协议播放的电影。

9.4.5 知识链接:TMG 用作 Internet 边缘防火墙

Forefront TMG 可以部署为专用 Internet 边缘防火墙,部署在连接内部网络与 Internet 的网络边缘,充当内部客户端的 Internet 安全网关。Forefront TMG 计算机对于通信路径上的其他方来说是透明的,Internet 用户应该无法判断此处是否有防火墙服务器,除非用户试图访问 Forefront TMG 计算机拒绝访问的网络服务、协议或站点。通过设置安全访问策略,管理员可以防止未经授权的访问和恶意内容进入网络,功能如下。

(1) 多层通信筛选——数据包级别、线路级别和应用程序级别筛选。
(2) 智能应用程序层警示应用程序筛选器。
(3) 内置入侵检测。
(4) 锁定基本操作系统的系统强化。

9.5 发布内部服务器

TMG 服务器在为局域网用户提供 Internet 连接共享的同时,也提供了防火墙功能,因为内网用户使用的都是私有 IP 地址,这样,外网用户就无法通过 IP 地址直接访问。但网络中通常需要搭建一些服务器向 Internet 提供服务,如 Web、E-mail 服务器等,这就需要利用 TMG 创建防火墙策略,将内部服务器发布到 Internet。

9.5.1 发布 Web 网站

利用 TMG 的"网站发布规则",可以将网络中的 Web 网站发布到 Internet。现在要将网站 www.coolpen.net 发布到 Internet,该网站的 IP 地址为 192.168.100.61。操作步骤如下。

(1) 在 Forefront TMG 控制台中,右击"防火墙策略"并选择快捷菜单中的"新建"→"网站发布规则"选项,启动"新建 Web 发布规则向导"。在"Web 发布规则名称"文本框为新规则设置一个名称,如图 9-61 所示。

(2) 单击"下一步"按钮,显示如图 9-62 所示的"请选择规则操作"对话框,选中"允许"单选按钮。

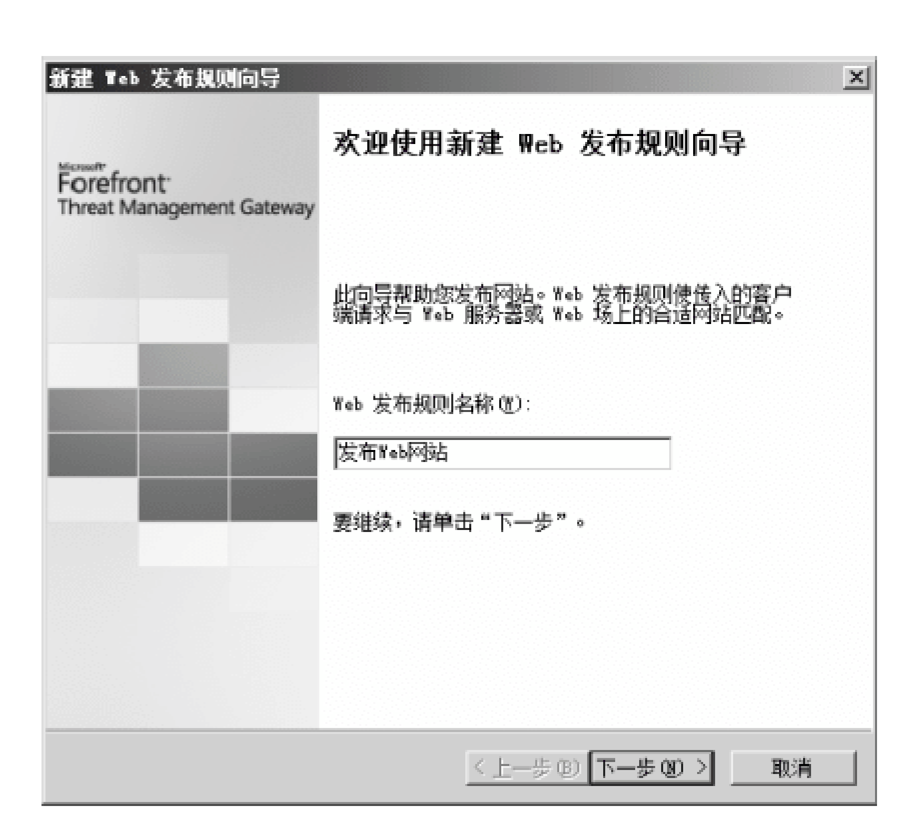


图 9-61 新建 Web 发布规则向导

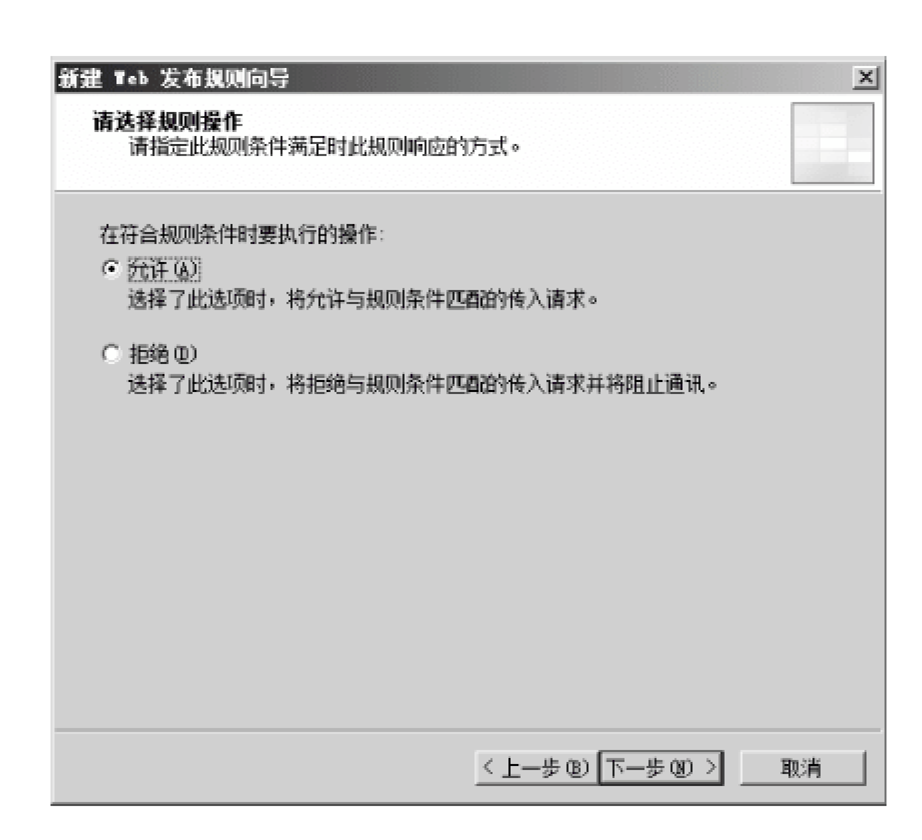


图 9-62 "请选择规则操作"对话框

(3) 单击"下一步"按钮,显示如图 9-63 所示的"发布类型"对话框。如果只发布一个网站或一个网站的群集服务器,可选中"发布单个网站或负载平衡器"单选按钮,这里选择该项;如果发布 Web 服务器上的多个站点,则选中"发布多个网站"单选按钮。

(4) 单击"下一步"按钮,显示如图 9-64 所示的"服务器连接安全"对话框,选中"使用不安全的连接连接发布的 Web 服务器或服务器场"单选按钮。

(5) 单击"下一步"按钮,显示如图 9-65 所示的"内部发布详细信息"对话框。在"内部站点名称"文本框中输入网站域名,如 www.coolpen.net,选中"使用计算机名称或 IP 地址

连接到发布的服务器”复选框，在“计算机名称或 IP 地址”文本框中输入 Web 服务器的计算机名称或 IP 地址。

（6）单击“下一步”按钮，显示如图 9-66 所示的“内部发布详细信息”对话框，在“路径（可选）”文本框中输入“/＊”。

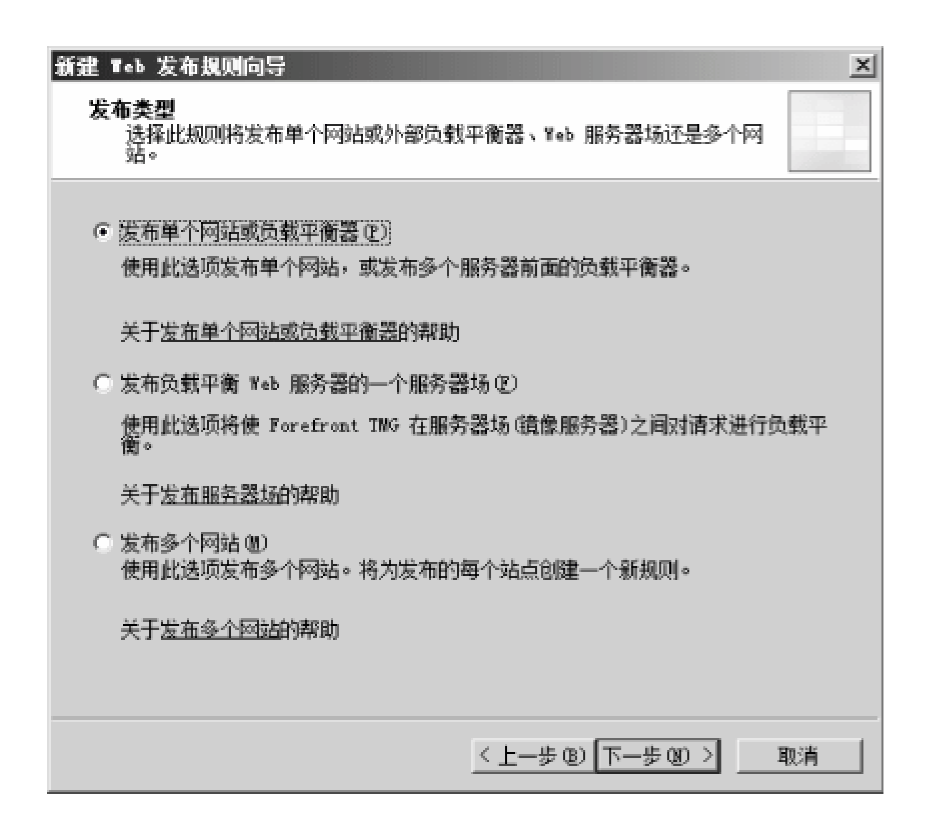


图 9-63 “发布类型”对话框



图 9-64 “服务器连接安全”对话框

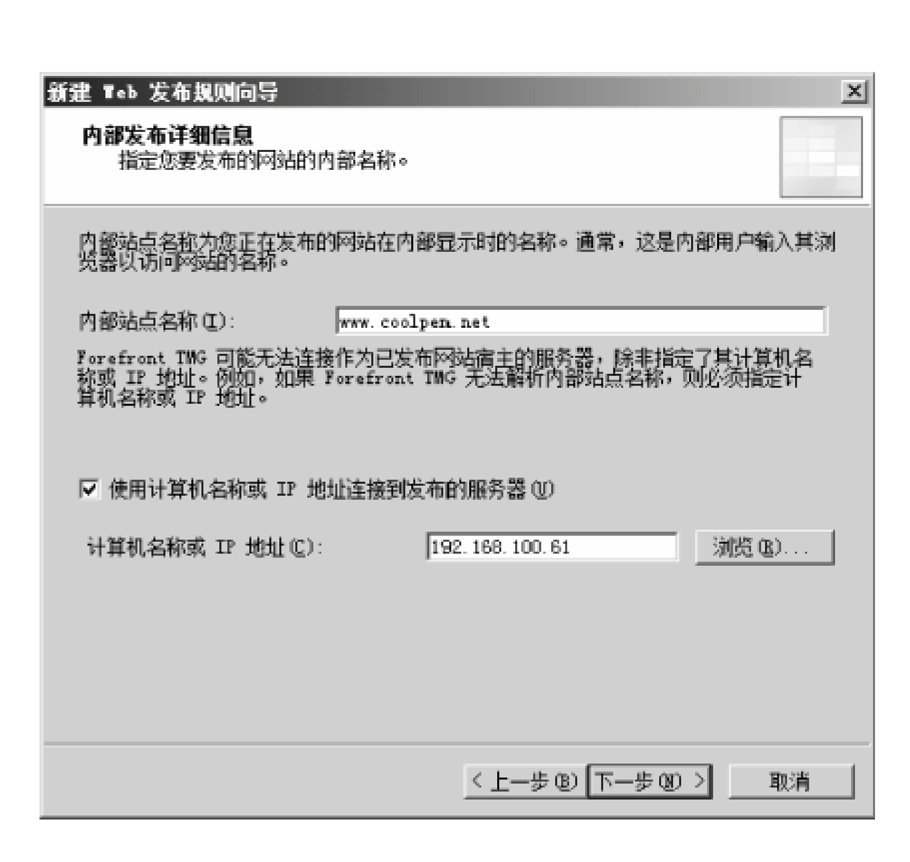


图 9-65 “内部发布详细信息”对话框

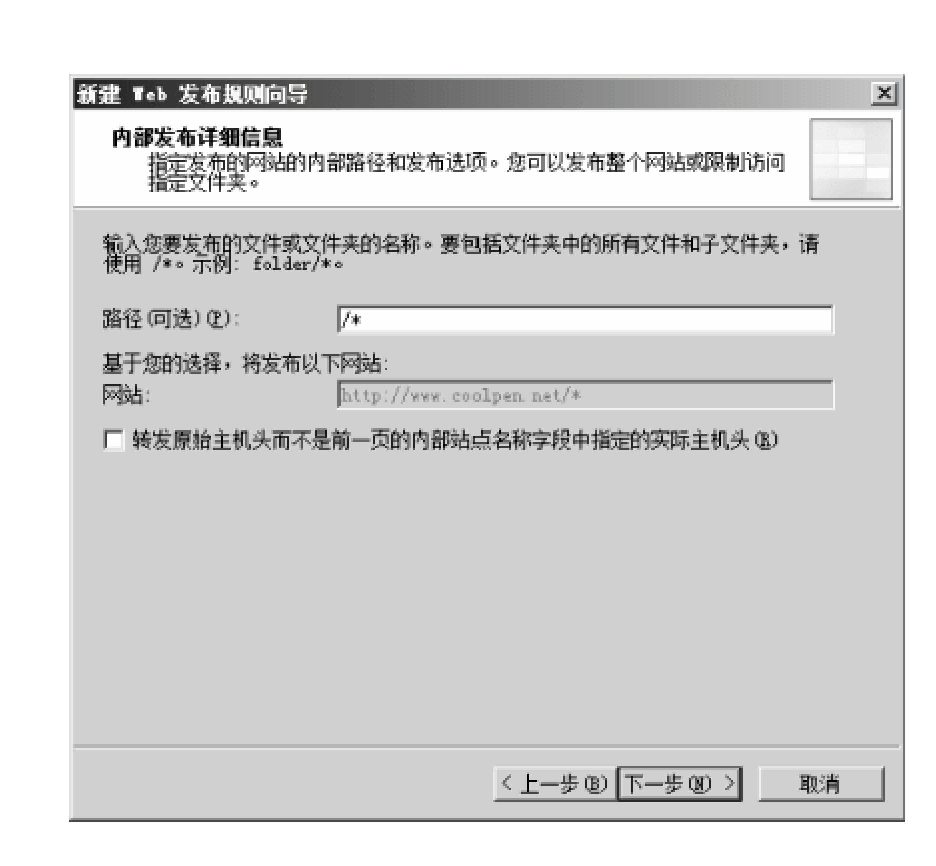


图 9-66 “内部发布详细信息”对话框

（7）单击“下一步”按钮，显示如图 9-67 所示的“公共名称细节”对话框。在“公用名称”文本框中，输入发布到 Internet 上的名称。

（8）单击“下一步”按钮，显示如图 9-68 所示的“选择 Web 侦听器”对话框。为发布的站点选择 Web 侦听器。在 Forefront TMG 中，每个绑定的 IP 地址（通常是 Internet 地址）都可以创建一个 Web 侦听器，并且选择该侦听器作为发布地址。默认情况下没有 Web 侦听器。

（9）单击“新建”按钮，启动“新建 Web 侦听器定义向导”。连续单击“下一步”按钮，在“Web 侦听器名称”文本框中输入一个名称，在“客户端连接安全设置”对话框中选中“不需要与客户端建立 SSL 安全连接”单选按钮，如图 9-69 所示。

（10）单击“下一步”按钮，显示如图 9-70 所示的“Web 侦听器 IP 地址”对话框，选择传入 Web 请求的网络。选中“外部”复选框。



图 9-67 “公共名称细节”对话框



图 9-68 “选择 Web 侦听器”对话框

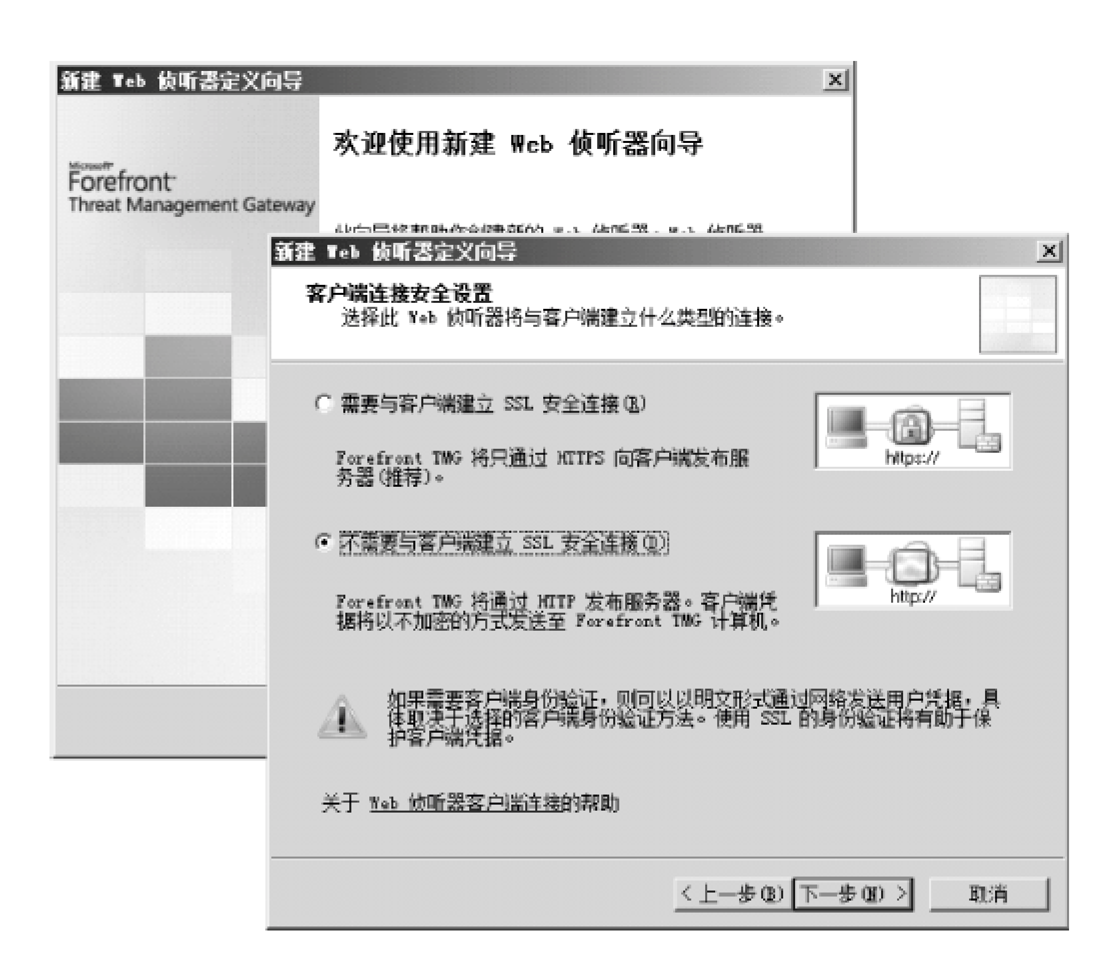


图 9-69 新建 Web 侦听器定义向导

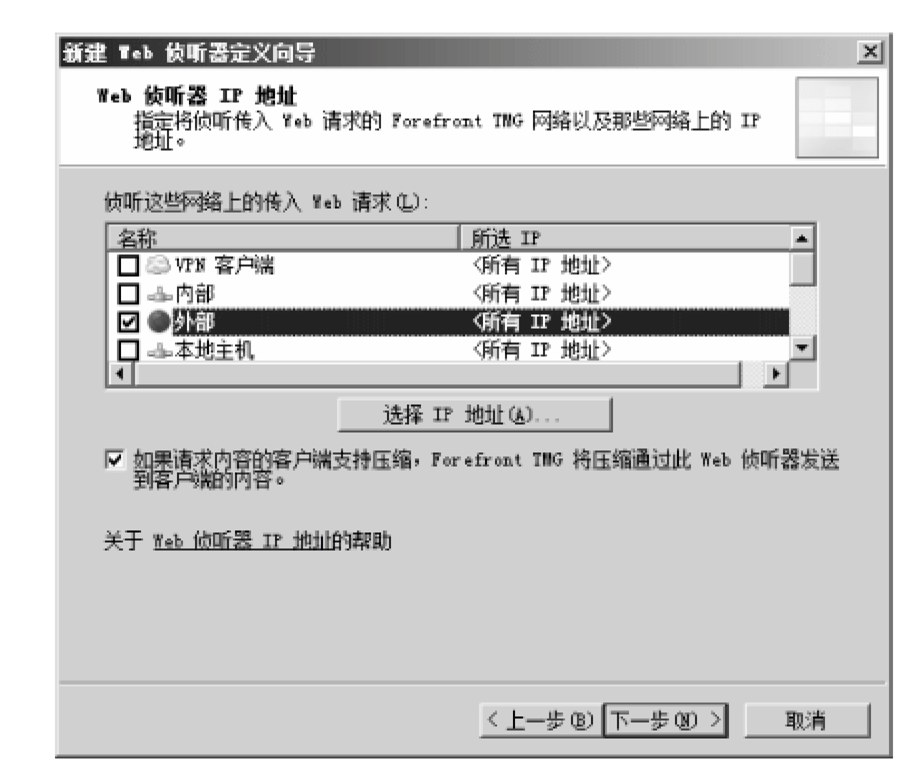


图 9-70 “Web 侦听器 IP 地址”对话框

(11) 单击“下一步”按钮，显示如图 9-71 所示的“身份验证设置”对话框。如果 Web 网站没有设置身份验证，在“选择客户端将如何向 Forefront TMG 提供凭据”下拉列表框中，选择“没有身份验证”选项即可。

(12) 连续单击“下一步”按钮，显示“正在完成新建 Web 侦听器向导”对话框，表示 Web 侦听器已经创建完成，如图 9-72 所示。

(13) 单击“完成”按钮返回“选择 Web 侦听器”对话框。在“Web 侦听器”下拉列表框中即可选择侦听器，如图 9-73 所示。如果内部网络有多个不同的 Web 网站，则需要创建多个 Web 侦听器。

(14) 单击“下一步”按钮，显示如图 9-74 所示的“身份验证委派”对话框，在下拉列表框中选择“无委派，客户端无法直接进行身份验证”选项。



图 9-71 “身份验证设置”对话框

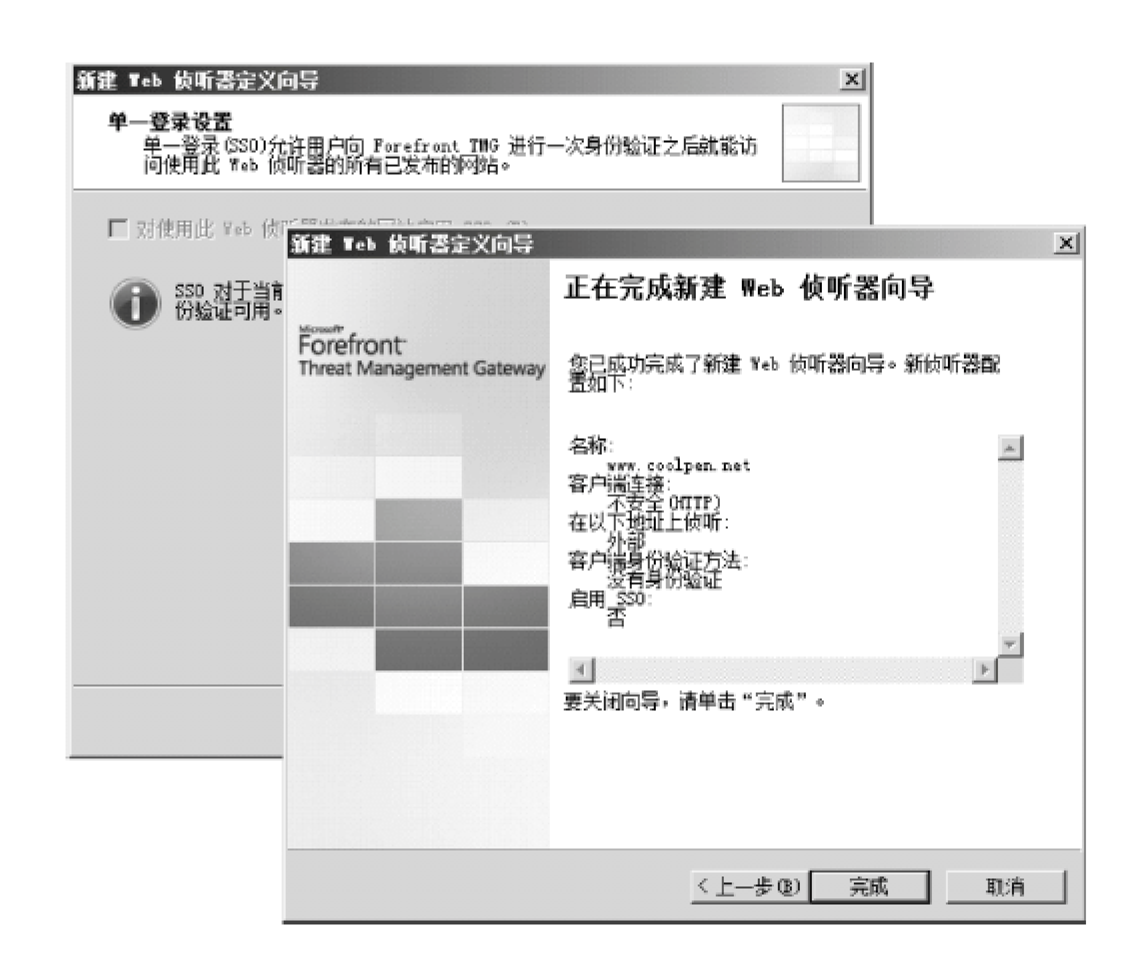


图 9-72 新建 Web 侦听器向导完成

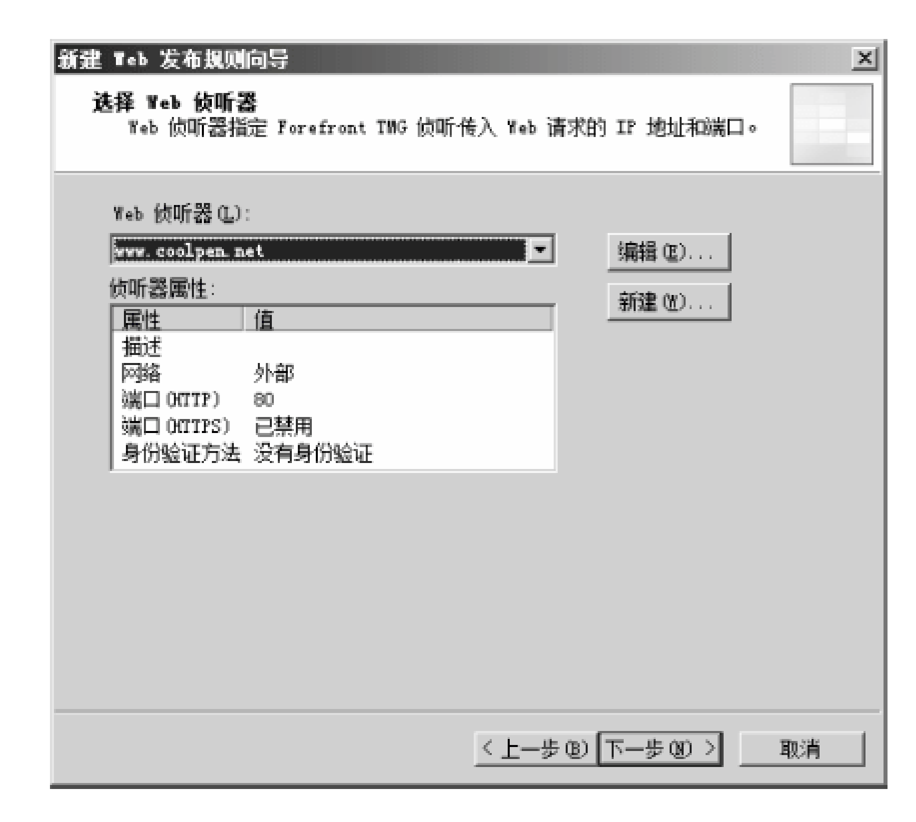


图 9-73 选择 Web 侦听器

（15）连续单击“下一步”按钮，在“用户集”对话框中使用默认设置即可；在如图 9-75 所示的“正在完成新建 Web 发布规则 向导”对话框，单击“完成”按钮。



图 9-74 “身份验证委派”对话框

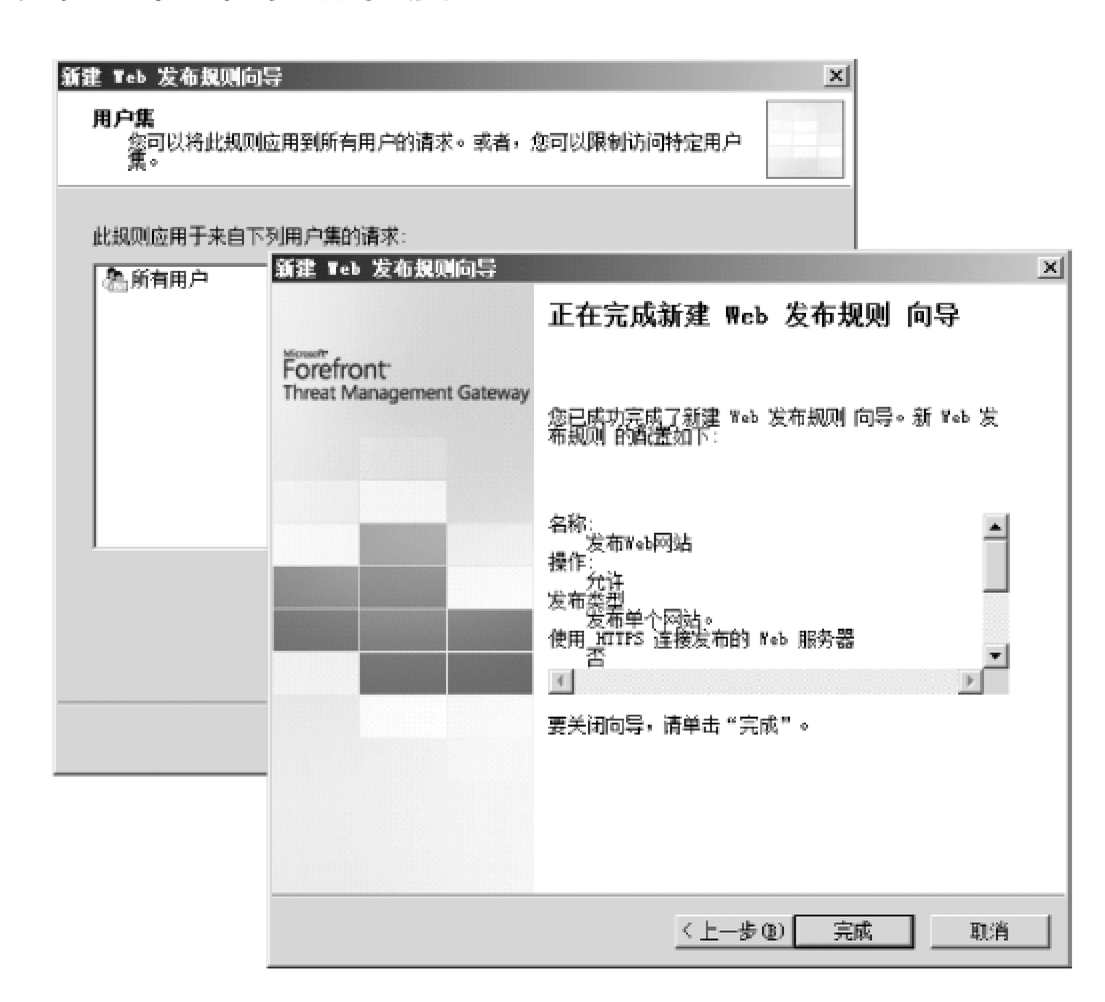


图 9-75 完成新建 Web 发布规则向导

（16）Web 发布规则创建完成后，需单击“应用”按钮便可使配置生效。

9.5.2 发布安全 Web 网站

安全 Web 站点使用 https://方式进行访问，并且默认使用 TCP 的 443 端口。在同一个 Web 服务器上，可以有多个使用 TCP 的 80 端口的普通 Web 站点，但只能有一个使用 TCP 的 443 端口的安全 Web 站点，如果想在一个 Web 服务器上提供多个安全 Web 站点，就要使用 TCP 的 443 之外的其他端口。

发布安全的 Web 网站时，和发布普通 Web 网站的操作步骤一样，只是在“服务器连接安全”对话框中，需选中“使用 SSL 连接到发布的 Web 服务器或服务器场”单选按钮，如图 9-76 所示。

需要注意的是，在 Forefront TMG 中，如果在同一个 Web 站点中既提供普通 Web 站点转发，又提供安全的 Web 站点转发，那么，就只能转发安全的 Web 站点，而不能提供普通的 Web 站点转发。

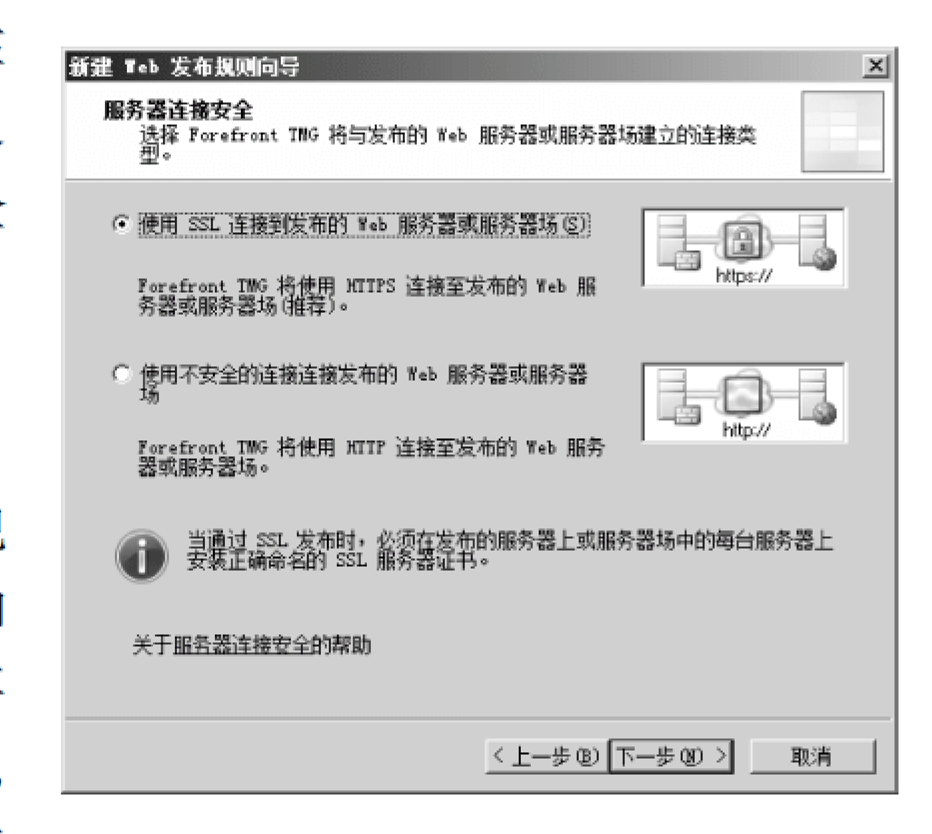


图 9-76　发布 HTTPS 服务器

9.5.3　发布邮件服务器

利用 Forefront TMG 的"邮件服务器发布规则"，可以将使用 SMTP、RPC、POP、IMAP 和 NNTP 协议的邮件服务器发布到 Internet。需要注意的是，由于邮件服务器不仅需要客户端访问，而且与 Internet 上的其他邮件服务器之间也需要转发邮件。因此，需要创建两个策略，一个是客户端访问；一个是服务器与服务器之间的通信。

(1) 在 Forefront TMG 控制台中，右击"防火墙策略"，在快捷菜单中依次选择"新建"→"邮件服务器发布规则"选项，启动"新建邮件服务器发布规则向导"。在"邮件服务器发布规则名称"文本框中输入一个名称，单击"下一步"按钮，显示如图 9-77 所示的"选择访问类型"对话框，选中"客户端访问：RPC、IMAP、POP3、SMTP"单选按钮。

(2) 单击"下一步"按钮，显示如图 9-78 所示的"选择服务"对话框，根据邮件服务器使用的协议，选择客户端的访问方式。



图 9-77　"选择访问类型"对话框

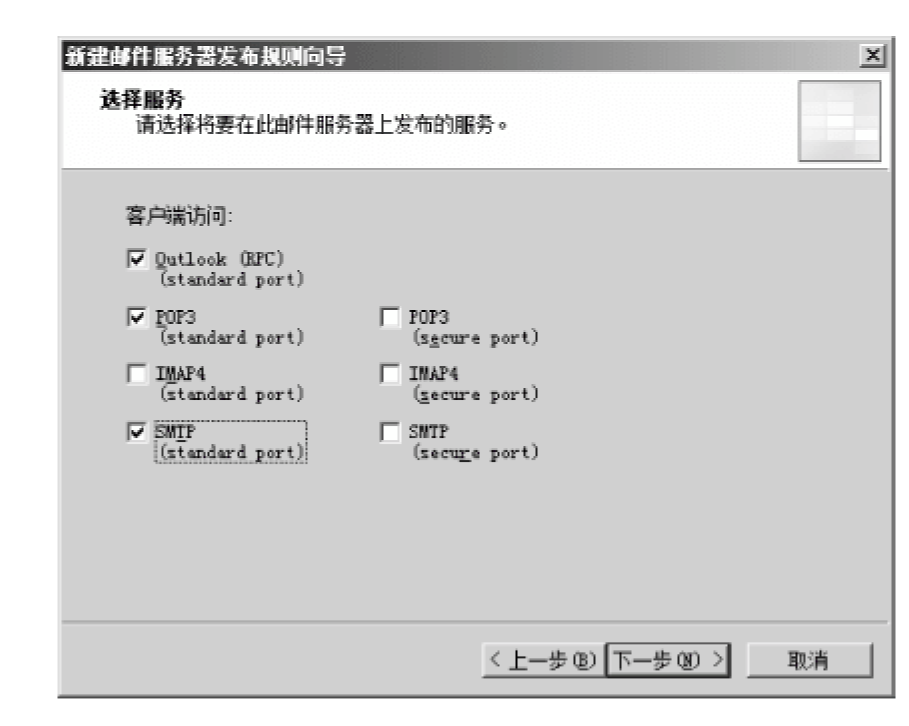


图 9-78　"选择服务"对话框

(3) 单击"下一步"按钮，显示如图 9-79 所示的"选择服务器"对话框。在"服务器 IP 地址"文本框中，输入要发布的内网邮件服务器的 IP 地址。

(4) 单击"下一步"按钮，显示"网络侦听器 IP 地址"对话框，选中"外部"复选框。单击"下一步"按钮，显示如图 9-80 所示的"正在完成新建 邮件服务器发布规则 向导"对话框。

(5) 单击"完成"按钮，邮件服务器发布完成。

此时，邮件服务器就可以通过 Forefront TMG 与 Internet 上的其他邮件服务器互相收发邮件，Internet 上的用户也可以使用 Foxmail、Outlook 等客户端程序收发邮件。不过，为




图 9-79 “选择服务器”对话框



图 9-80 完成新建邮件服务器发布规则向导

了使邮件服务器之间能够通信，还应创建一条规则，用于发布 SMTP 服务。再次运行“新建邮件服务器发布规则向导”，在“选择访问类型”对话框中，选中“服务器到服务器的通讯：SMTP、NNTP”单选按钮；在“选择服务”对话框中选中 SMTP 复选框即可，如图 9-81 所示。

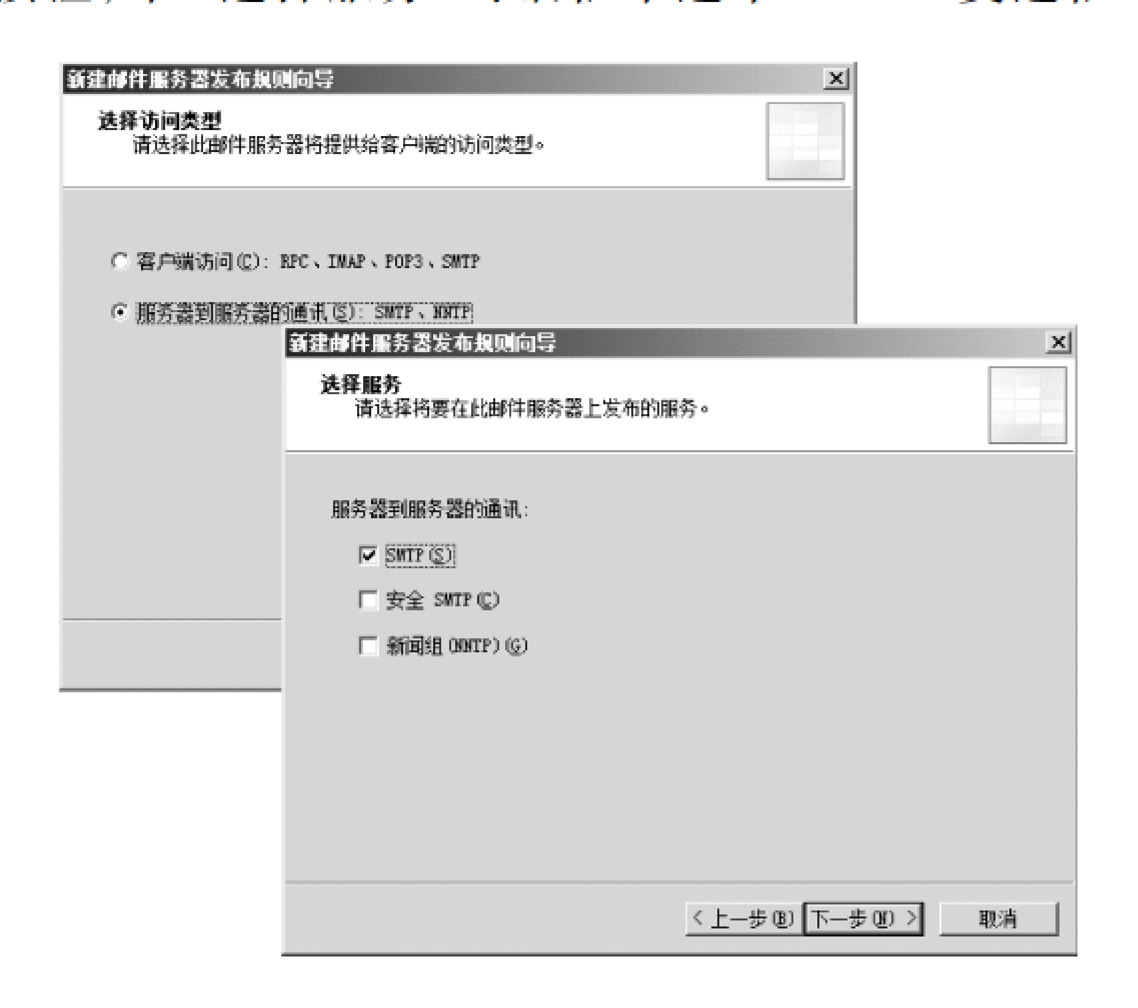


图 9-81 发布 SMTP 服务器

9.5.4 发布 Exchange Web 客户端访问

如果邮件服务器使用 Exchange 2000、Exchange Server 2003 或 Exchange Server 2007 搭建，那么，除了发布邮件服务器以外，还要发布 Exchange 的 Web 客户端访问。

(1) 在 Forefront TMG 控制台中，右击“防火墙策略”，从快捷菜单中选择“新建”→“Exchange Web 客户端访问发布规则”选项，启动“新建 Exchange 发布规则向导”。

(2) 单击“下一步”按钮，显示“选择服务”对话框，在“Exchange 版本”下拉列表框中选择 Exchange 版本，在“Web 客户端邮件服务”选项组中选中 Outlook Web Access 复选框，如图 9-82 所示。

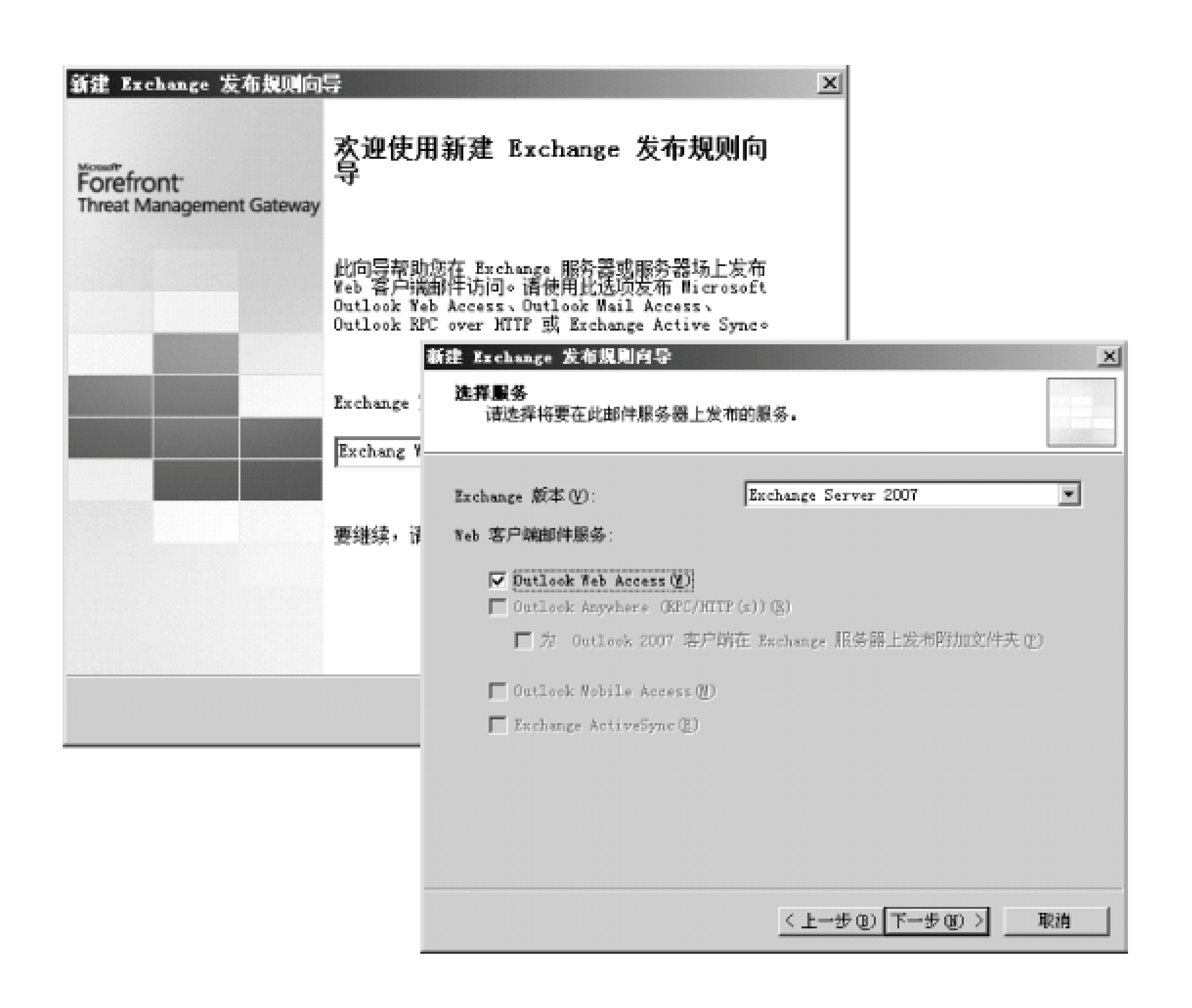


图 9-82 “选择服务”对话框

(3) 连续单击“下一步”按钮,在“发布类型”对话框中选中“发布单个网站或负载平衡器”单选按钮。在“服务器连接安全”对话框中选中“使用不安全的连接连接发布的 Web 服务器或服务器场”单选按钮,如图 9-83 所示。

(4) 单击“下一步”按钮,显示“内部发布详细信息”对话框。在“内部站点名称”文本框中,输入内部 E-mail 站点的名称,例如 mail. coolpen. net;选中“使用计算机名称或 IP 地址连接到发布的服务器”复选框,在“计算机名称或 IP 地址”文本框中,输入邮件服务器的计算机名称或 IP 地址,如图 9-84 所示。




图 9-83 “服务器连接安全”对话框

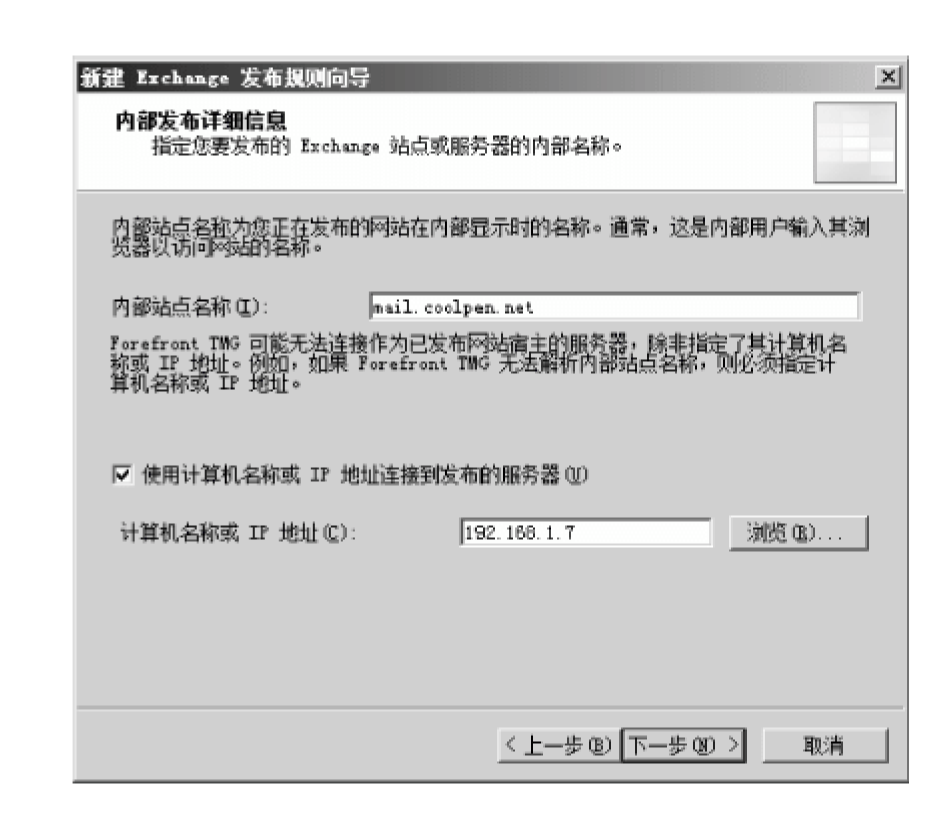


图 9-84 “内部发布详细信息”对话框

(5) 单击“下一步”按钮,显示如图 9-85 所示的“公共名称细节”对话框。在“接受请求”下拉列表框中,选择“此域名(在以下输入)”选项;在“公用名称”文本框中,输入邮件服务器的域名,例如 mail. coolpen. net。

(6) 单击“下一步”按钮，在“客户端连接安全设置”对话框中，要选中“需要与客户端建立 SSL 安全连接”单选按钮，并单击“下一步”按钮，在“侦听器 SSL 证书”对话框中选择 SSL 证书，如图 9-86 所示。



图 9-85　“公共名称细节”对话框



图 9-86　选择 SSL 证书

(7) 单击“下一步”按钮，显示“选择 Web 侦听器”对话框。需要创建一个侦听器，用来指向 Exchange Web 服务器的 IP 地址。由于 Exchange OWA 采用 HTTPS 方式，因此，所创建的侦听器也应该使用 HTTP 方式，如图 9-87 所示。

(8) 连续单击“下一步”按钮，在“身份验证委派”对话框的下拉列表框中，选择“无委派，客户端无法直接进行身份验证”选项。在“正在完成新建 Exchange 发布规则 向导”对话框中单击“完成”按钮即可，如图 9-88 所示。



图 9-87　“选择 Web 侦听器”对话框

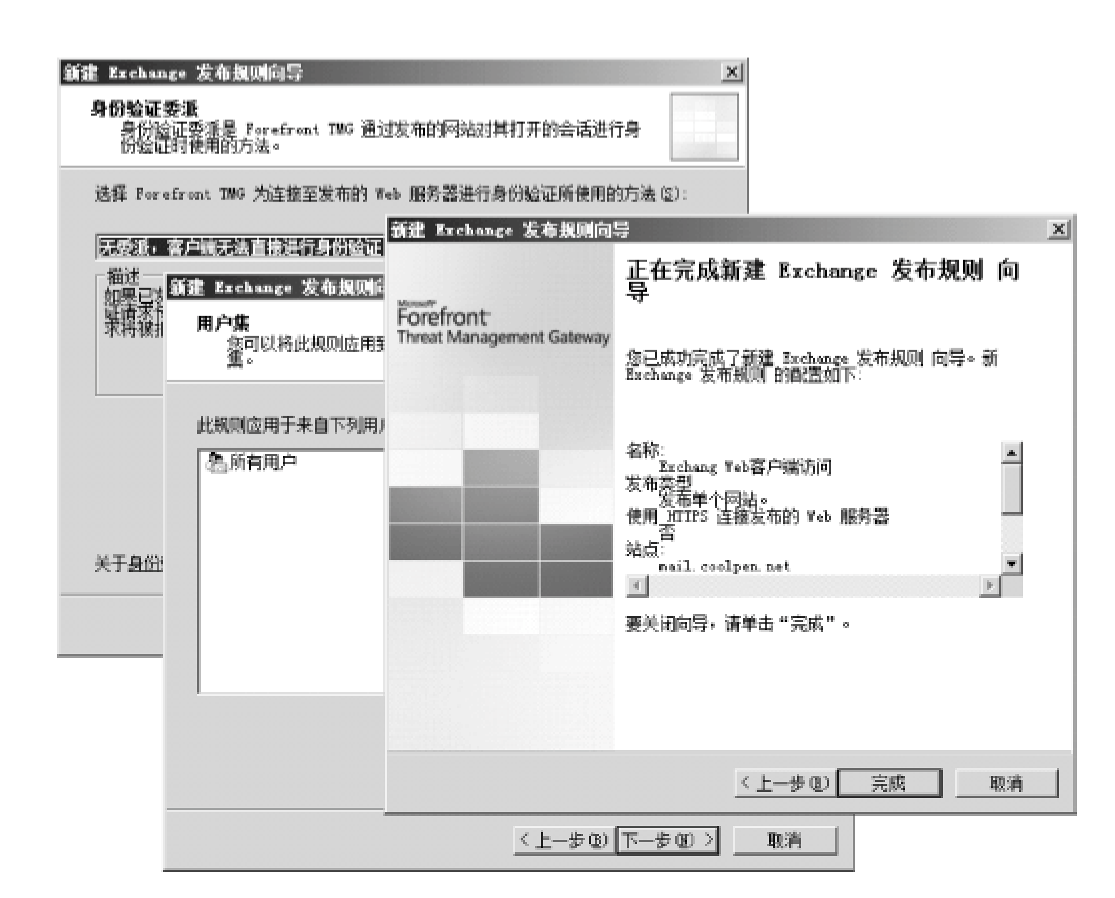


图 9-88　规则创建完成

(9) 单击“应用”按钮，使设置生效即可。

9.5.5　知识链接：服务器发布

公司网络通常也需要向 Internet 提供服务，如 Web 网站、电子邮件服务等。因此，

Forefront TMG 也提供了发布服务器功能,可以在不危及内部网络安全的情况下将服务发布到 Internet。组织可以配置 Web 发布规则和服务器发布规则,来确定哪些请求向下游发送到位于 TMG 服务器防火墙后的服务器,以便为内部服务器提供增强的安全层。所有转发的通信对 TMG 服务器的监控状态筛选和检测引擎都是公开的。

例如,Microsoft Exchange 服务器可以放置在 TMG 服务器后,可以创建服务器发布规则,来允许对 Exchange 简单邮件传输协议(SMTP)、POP3、Internet 邮件访问协议(IMAP4)和网络对网络传输协议(NNTP)服务进行 SSL 保护的远程访问。Forefront TMG SMTP 消息筛选程序对传入到 Exchange 服务器的电子邮件进行侦听。然后,Forefront TMG SMTP 消息筛选程序可以对 SMTP 通信进行筛选,并将它转发给 Exchange 服务器。Exchange 服务器从不直接对外部用户公开,而是保留在安全的环境中,维护对其他内部网络服务的访问,具有以下功能。

(1) 简便的安全服务器发布向导。

(2) 用于透明客户端连接和服务器发布的 SecureNAT。

(3) 已发布的服务,包括超文本传输协议/安全套接字层(HTTP/SSL)、FTP、SMTP、POP3、IMAP4、NNTP、DNS、RDP、H.323、流媒体等。

习题

1. 简述 Forefront TMG 的主要功能。
2. Forefront TMG 服务器将网络分割为哪几部分?是如何实现安全防护的?
3. 如何通过 TMG 服务器禁止某些用户访问 Internet?
4. 如何将内网服务器发布到 Internet?

实验:禁止内部用户访问危险网站

实验目的:

掌握如何通过 TMG 服务器控制内网安全访问 Internet。

实验内容:

通过 TMG 服务器阻止部分用户访问指定的 Web 站点。

实验步骤:

(1) 在企业网络边缘部署 TMG 服务器。

(2) 在域控制器上创建用于实验测试的用户组,并将测试账户添加到组中。

(3) 在 TMG 服务器上创建域名集,并将禁止访问的 Web 站点域名添加到域名集中。

(4) TMG 服务器的防火墙策略中新建访问规则,限制指定用户组访问域名集中的 Web 站点。

(5) 使用测试用户账户登录网络,尝试访问被禁止的 Web 站点,验证实验效果。

第 10 章 chapter 10

远程接入安全

远程访问是大多数企业网络的必备功能，员工出差、在家办公、分支部门与总部网络共享资源等都离不开远程访问。VPN（Virtual Private Network，虚拟专用网）是目前常用的远程访问技术之一，主要特点就是安全可靠，机制灵活，费用低廉，易于实现。Windows 系统内置了 VPN 客户端组件，客户端只需经过简单配置，借助 Internet 即可拨叫到 VPN 服务器，访问内网资源。

10.1 远程安全接入规划

目前广泛应用的 VPN 都是基于 Internet 的，而 Internet 是高度开放的，因此，安全性仍然是 VPN 用户最关注的问题。通常情况下，VPN 主要采用 4 项技术来保证通信安全，分别是隧道技术（Tunneling）、加解密技术（Encryption and Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。部署安全接入系统之前，必须结合实际需要选择适当的安全接入方式。

10.1.1 案例情景

该企业在外地有两家分支机构，每天都要将当天的业务数据传回到总部网络。由于总部网络和分支网络都已经接入 Internet，因此通常都是通过 E-mail 或即时消息软件将数据信息传输到总公司。其实，这种方式存在很大的安全隐患。E-mail 邮箱的安全性是很低的，尤其是一些意义重大的机密数据，绝对不可以通过 E-mail 传输，甚至绝对不能接触到 Internet。至于即时消息软件的安全性就更差了，不仅无法对通信双方的身份进行验证，而且传输过程都是未经加密的，传输数据很容易被截获和篡改。

目前该企业总部网络采用 100Mbps 光纤线路接入 Internet，网络中的所有计算机均经过防火墙连接到 Internet。两家分支机构的计算机数量在 30 台左右。鉴于大部分内部信息资源的特殊性和机密性，对用户身份认证、传输过程具有较高的可靠性和可控性要求，因此该公司计划利用 VPN 技术组建虚拟网。

10.1.2 项目需求

远程访问 VPN 系统主要包括 VPN 服务器和 VPN 客户端。对于该项目而言，VPN 服务器需要部署在企业总部网络，Windows Server 2008 服务器、路由器、防火墙等都可以提

供 VPN 服务器功能。至于 VPN 客户端则对分支网络用户没有特殊要求。为了确保通信安全，需要采取 SSL、IPSec 等安全措施，确保远程访问 VPN 链接的可靠性和机密性。鉴于当前的实际情况和需求，部署的 VPN 系统将满足如下要求。

1. 安全连接，多种验证技术

支持细化的权限管理，可以单独设置某台计算机或某用户能或不能访问指定的资源或指定的服务。支持用户与计算机绑定(硬件授权、定机定人)、USB KEY、可选一次性口令或短信认证等，有效防范移动客户端扩散失控；支持客户端计算机之间相互访问，客户端计算机接入 VPN 后禁止访问 Internet。

2. 运行稳定，高效可靠

为保证 VPN 业务实时处理和连续工作，中心 VPN 网关(VPN 服务器或者硬件设备)要求确保网络系统的正常连通。

3. 升级和扩展性

网络设备应能快速适应各分支机构接入的动态增减，并在增减过程中，对已部署好的分支机构及移动客户端没有影响，同时考虑未来的业务模式增长，要求设备支持软硬件的扩展升级。

4. 性能优化

中心 VPN 网关(VPN 服务器或者硬件设备)能够通过业务分类和定义优先级别，实现智能化的拥塞控制、QoS 功能。

5. 智能化网络管理

企业总部能对各分支 VPN 网关(如有)集中控制、集中管理、集中监控、远程维护，以节省管理和维护成本。

6. 业务系统应用模式

集团部署的业务系统中，部分采用 C/S 结构模式，例如新闻业务处理系统，该业务系统和 Windows Server 2008 Active Directory 结合，同时结合 Windows 身份验证模式访问数据库，部署的 VPN 系统将支持该业务应用模式。

网络中部署网络防病毒系统，VPN 客户端计算机可以使用总部防病毒服务器进行自动升级。总部与分支机构之间的计算机可以相互访问，通过 NETBIOS 名实现相互的访问和数据传输。可以实时访问总部的网络资源以及数据库系统。

7. 支持断线重拨技术

为了保证拨号网络的稳定性，VPN 设备集成自动拨号软件，在拨号中断后，5s 内可以重拨。网络物理连接恢复正常后，VPN 隧道将在 1min 内自动建立，从而保证系统迅速恢复。

VPN 系统部署成功后，以 VPN 网络为基础，将企业总部、分支机构和移动用户连接成为一个局域网，轻松实现数据流实时同步和远程办公、文件共享等功能。局域网内的所有应用都可以扩展到远程分支机构和移动用户，从而真正实现了企业范围内的系统共享化和信息一体化。

10.1.3 解决方案

目前，企业总部拥有 100Mbps 光纤接入 Internet 的基础环境，并且拥有多个公网 IP 地

址；总部网络设备架构相当完善，通过 Cisco 三层交换机实现合理的子网划分和跨网段管理功能。

1. 拓扑结构

总部网络 VPN 服务器的 WAN 口配置一个单独的公网 IP 地址，内网接口连接至内网交换机上。分支机构中的 VPN 客户端用户可以通过 Internet 连接拨叫到 VPN 服务器，从而建立隧道连接。通过在 VPN 服务器上配置静态路由和扩大 IPSec 子网掩码功能，使所有远端客户端计算机对总部所有 VLAN 的数据访问均可以通过三层交换机 IP 到达，实现基于 IPSec 协议的双向隧道通信；总部所有客户端计算机对互联网的访问，仍通过现有的防火墙做数据转发。

其他分支机构及出差的移动用户，通过在计算机上安装 VPN 客户端软件或使用 SSL 协议，只要可以访问 Internet，就可以安全地接入总部内网，与相应的服务器、客户端计算机之间实现双向数据访问。远程接入 VPN 的实现方式有多种，在当前企业网络中，可以借助路由器和防火墙实现，也可以通过搭建专用 VPN 服务器实现。图 10-1 所示为搭建专用 VPN 服务器时的网络拓扑结构。

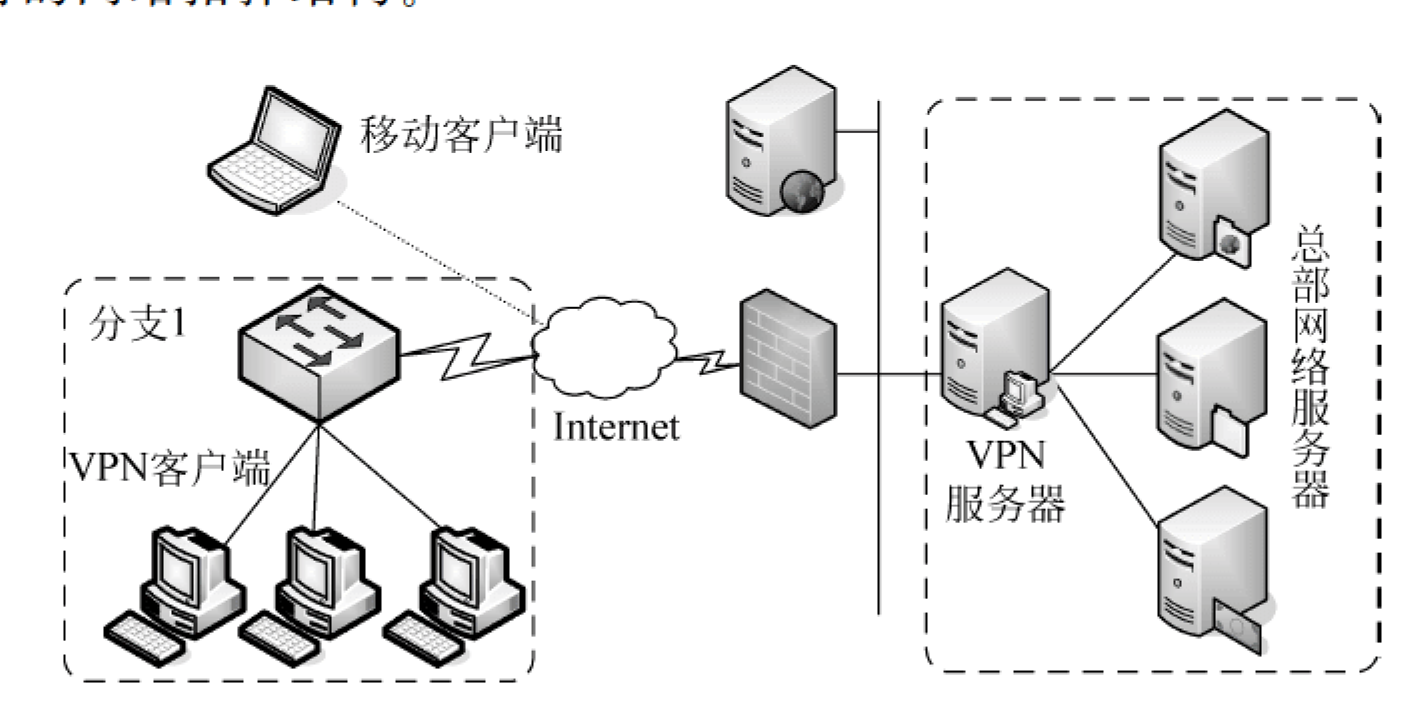


图 10-1　VPN 系统拓扑结构

2. VPN 协议的选择

Windows Server 2008 支持如下远程访问 VPN 协议。

(1) PPTP：PPTP 使用 PPP 用户身份验证和 MPPE 加密。当使用具有强壮密码的 MS-CHAP v2 或 PEAP-MS-CHAP v2 时，PPTP 是一种安全的 VPN 技术。对于基于证书的身份验证，EAP-TLS 可与基于注册的证书或智能卡一同使用。PPTP 被广泛支持，易于配置，可用于大部分网络地址转换(NAT)。Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP 均支持 PPTP。

(2) L2TP/IPSec：L2TP 利用 PPP 用户身份验证和 IPSec 数据包保护。L2TP/IPSec 使用证书(默认)和 IPSec 计算机级的身份验证过程来协商受保护的 IPSec 会话，然后基于 PPP 的用户身份验证来认证 VPN 客户端计算机的用户。通过使用 IPSec，L2TP/IPSec 为每个数据包提供了数据机密性(加密)、数据完整性(证明数据没有在传输过程中被修改)和数据的原始认证(证明数据由授权用户发出)。但是 L2TP/IPSec 需要 PKI 为每个基于 L2TP/IPSec 的 VPN 客户端分配计算机证书。Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP 均支持 L2TP/IPSec。

(3) SSTP：SSTP 利用 PPP 用户身份验证，为封装和加密使用 SSL 上的 HTTP 通道。

因为 SSTP 使用 SSL 通信(使用 TCP 端口 443),所以 SSTP 可用于多种不同的网络配置,如位于 NAT、防火墙或不支持 PPP 或 L2TP/IPSec 通信的代理服务器之后的 VPN 客户端或服务器。只有 Windows Server 2008 和 Windows Vista SP1 支持 SSTP。

为远程 VPN 连接选择加密协议时,应遵循如下原则。

(1) 当使用 PEAP-MS-CHAP v2、EAP-MS-CHAP v2 或 MS-CHAP v2 身份验证时,PPTP 不需要证书基础结构来为每个 VPN 客户端发布证书。

(2) 基于 PPTP 的 VPN 连接为数据包提供数据机密性(加密)。基于 PPTP 的 VPN 连接不提供数据完整性或数据原始认证。

(3) 通过使用 IPSec,基于 L2TP/IPSec 的 VPN 连接提供数据机密性、数据完整性和数据原始认证。

(4) 基于 SSTP 的 VPN 连接客户端和服务器可置于 NAT、防火墙或 Web 代理之后。但是,SSTP 不支持位于身份验证 Web 代理之后的 VPN 客户端和服务器。

(5) 默认情况下,运行 Windows Server 2008 的 VPN 服务器同时支持这 3 种 VPN 连接类型。对于没有安装计算机证书的 VPN 客户端,用户可以使用 PPTP。对于安装了计算机证书的 VPN 客户端,用户可以使用 L2TP/IPSec。对于运行 Windows Vista SP1 的 VPN 客户端使用 SSTP。

(6) 如果用户正在联合使用 VPN 协议,用户可以为 PPTP、L2TP/IPSec 或 SSTP 连接创建单独的网络策略,定义不同的连接设置。

(7) 在 Windows Server 2008 和 Windows Vista 中,IPv6 通信可通过基于 PPTP 的 VPN 连接作为 IPv4 隧道通信进行发送,或者在 VPN 隧道中进行本地 IPv6 通信。

(8) 在 Windows Server 2008 和 Windows Vista 中,L2TP/IPSec 或 SSTP 的 VPN 连接支持作为 IPv4 隧道通信的 IPv6 通信、VPN 隧道内的 IPv6 通信,以及 IPv6 之上的 VPN 连接。

3. VPN 服务器

基于 Windows Server 2008 系统远程访问功能的 VPN 连接,有如下配置要求。

(1) VPN 服务器的 Internet 接口和内网接口必须拥有静态 IP 地址。由于默认路由冲突的可能性,用户应该使用 IPv4 地址手动配置内网接口、子网掩码、DNS 服务器和 WINS 服务器。但是,不要配置 VPN 服务器内网接口的默认网关。这样才可能使 VPN 服务器拥有手动 TCP/IP(IPv4)配置,并且使用 DHCP 获取 IPv4 地址。

(2) 对于使用 PEAP-MS-CHAP v2、EAP-TLS 或 PEAP-TLS 身份验证协议的 VPN 连接,用户必须在身份验证服务器上安装 VPN 客户端可以验证的计算机证书。用户也可能需要在 VPN 客户端上安装身份验证服务器的计算机证书的发行 CA 的根 CA 证书。

(3) 对于基于 SSTP 的 VPN 连接,用户必须在 VPN 服务器上安装 VPN 客户端可以验证的计算机证书。用户也可能需要在 VPN 客户端上安装 VPN 服务器的计算机证书的发行 CA 的根 CA 证书。

(4) 对于基于 L2TP/IPSec 的 VPN 连接,用户必须在 VPN 服务器上安装 VPN 客户端可以验证的计算机证书。

(5) 如果用户为本地身份验证或为 RADIUS 身份验证配置 VPN 服务器,并且 RADIUS 服务器是运行 NPS 的计算机,则默认网络策略将会拒绝所有类型的连接尝试,除非远程访问允许的用户账户拨号属性允许访问的。如果用户想要为 VPN 连接使用该网络

策略，则设置策略类型为“允许访问”。如果用户想要通过组或连接类型管理授权和 VPN 连接设置，则用户必须配置其他 NPS 策略。

4. VPN 客户端

部署 VPN 客户端时应遵循如下原则。

(1) 如果 VPN 客户端数量较少，则可以在每台计算机上执行 VPN 连接的手动配置。

(2) 如果 VPN 客户端数量较多，或者分别运行不同 Windows 版本，则建议使用 Windows Server 2008 的 CM 组件创建包含 VPN 配置设置的 CM 配置文件，并且对于拨号连接，需要维护电话簿数据库。

(3) 对于 L2TP/IPSec 连接，用户必须在 VPN 客户端计算机上安装计算机证书。

(4) 对于 PEAP-TLS 或 EAP-TLS 身份验证方式，用户必须在 VPN 客户端上安装用户证书，或者为用户发布智能卡。

(5) 对于 SSTP 连接，用户必须确保 VPN 客户端安装了 VPN 服务器的计算机证书的发布 CA 的根 CA 证书。

(6) 对于 PEAP-MS-CHAP v2 或 PEAP-TLS 身份验证方式，如果 VPN 客户端验证了认证服务器的证书(推荐)，那么用户必须确保 VPN 客户端安装了身份验证服务器的计算机证书的发布 CA 的根 CA 证书。

5. VPN 客户端的内网和 Internet 并存访问

默认情况下，当基于 Windows 的 VPN 客户端建立 VPN 连接时，会自动为 VPN 连接添加新的默认路由，并且修改现有默认路由，即断开客户端计算机到 VPN 服务器之外的所有其他 Internet 连接。为了防止创建新的默认路由，用户可以配置 VPN 连接不使用远程网络的默认网关。

(1) 在“控制面板”的“网络连接”窗口中，右击 VPN 网络连接并选择“属性”选项，显示“VPN 连接 属性”对话框，切换到“网络”选项卡中，双击“Internet 协议版本(TCP/IPv4)”项目，显示“Internet 协议版本 4(TCP/IPv4)属性”对话框，如图 10-2 所示。

(2) 单击“高级”按钮，显示“高级 TCP/IP 设置”对话框。在“IP 设置”选项卡中，取消选中“在远程网络上使用默认网关”复选框即可，如图 10-3 所示。

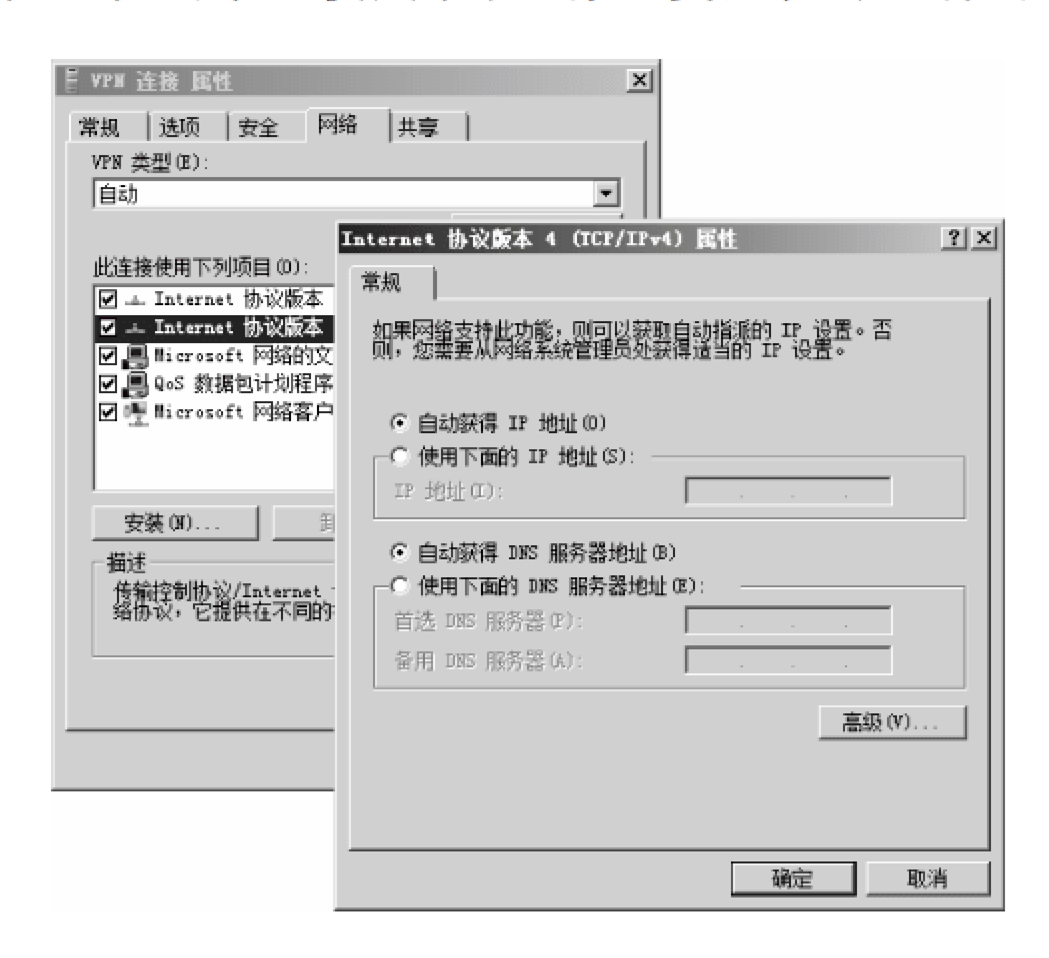


图 10-2 “Internet 协议版本 4(TCP/IPv4)属性”对话框

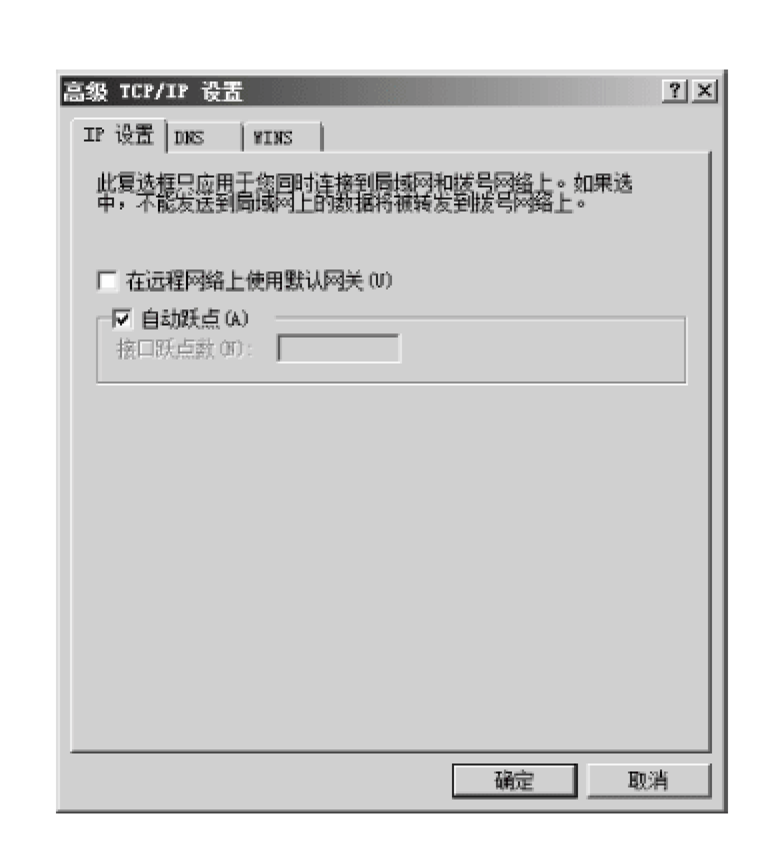


图 10-3 “高级 TCP/IP 设置”对话框

经过上述设置后,在建立连接时将不会创建默认路由。但是,符合分配 IPv4 地址的 Internet 地址类的路由将会被创建。例如,如果分配的地址为 10.0.12.119,那么基于 Windows 的 VPN 客户端会使用子网掩码 255.0.0.0 为地址前缀 10.0.0.0 创建路由。

“在远程网络上使用默认网关”选项的功能如下。

(1) 如果取消此复选框,则客户端计算机连接到 VPN 服务器时仍可以访问 Internet,除了符合分配 IP 地址的地址类的可以到达内网,其他不可到达内网。

(2) 如果选中此复选框,则所有内网位置都可到达,除了 VPN 服务器的地址和通过其他路由的可以到达 Internet,其他不可到达 Internet。

对于大部分连接 Internet 的 VPN 客户端,这种行为不能说明问题,因为它们通常参与内网或 Internet,而不是参与这两者。因此,系统默认选中“在远程网络上使用默认网关”复选框。对于需要并存访问内网和 Internet 资源的 VPN 客户端,用户可以完成如下操作之一。

(1) 选中“在远程网络上使用默认网关”复选框,并且允许通过企业内网访问 Internet。在 VPN 客户端和 Internet 主机之间的 Internet 通信将会穿过防火墙或代理服务器。尽管在性能上会有所影响,但是当 VPN 客户端连接着企业网络时,这种方式允许 Internet 访问被筛选,并且根据企业网络策略进行监视。

(2) 如果内网中的 IPv4 寻址是根据单一分类的地址前缀,则可以取消选中“在远程网络上使用默认网关”复选框。

(3) 如果内网中的 IPv4 寻址不是根据单一分类的地址前缀,则用户可以使用如下解决方式。

① 无等级静态路由 DHCP 选项。

② 连接管理工具。

③ 在 VPN 客户端上的命令文件。

10.2 安装和配置 Windows VPN

Windows Server 2008 系统已经集成了路由和远程访问功能,用户只需稍加配置即可用作 VPN 服务器,并且 Windows 系统用户还可以通过创建相应的 VPN 专用网络连接,成为 VPN 客户端。这种 VPN 实现方式操作简便,投资最少,是广大中小企业网络用户的首选。

10.2.1 前期准备工作

部署远程安全访问 VPN 系统需要用到域控制器、证书服务器等基本组件,实施之前必须做好各项准备工作。

1. 准备域环境

在网络中准备域控制器,证书服务器、安全策略服务器等可以部署在其他成员服务器上。

2. 设置 IP 地址

VPN 服务器需要安装两块网卡,一块用来连接局域网;另一块用来连接 Internet,供远程用户拨局域网。将连接局域网的本地连接,设置局域网 IP 地址,如图 10-4 所示。DNS 服务器设置为域控制器的 IP 地址,用来加入域。

将另一个连接 Internet 的本地连接的 IP 地址设置为 Internet 上有效的 IP 地址,如图 10-5 所示。



图 10-4　设置内网 IP 地址



图 10-5　设置外网 IP 地址

3. 加入域

配置 VPN 远程访问之前，应将 VPN 服务器加入到域。首先将 VPN 服务器的 DNS 服务器地址指向域控制器，然后在“服务器管理器”窗口中，单击“更改系统属性”链接，显示“系统属性”对话框。在“计算机名”选项卡中，单击“更改”按钮，显示如图 10-6 所示的“计算机名/域更改”对话框，选中“域”单选按钮，并输入域名。单击“确定”按钮，显示“Windows 安全”对话框，在“用户名”和“密码”文本框中，输入具有加入域权限的用户名和密码即可。

单击“确定”按钮即可加入域。根据系统提示重新启动系统，使用域用户账户登录即可。

4. 安装并设置 DHCP 服务器

当远程客户端拨入局域网以后，需要获得相应的局域网 IP 地址，才能访问局域网中的资源。因此，需要在网络中部署 DHCP 服务器，创建作用域并启用网络访问保护。需要注意的是，一定要进行授权，否则无法向客户端分配 IP 地址。另外，如果不想安装 DHCP 服务器，也可以在配置“路由和远程服务器”的过程中设置分配给客户端的 IP 地址范围。



图 10-6　“计算机名/域更改”对话框

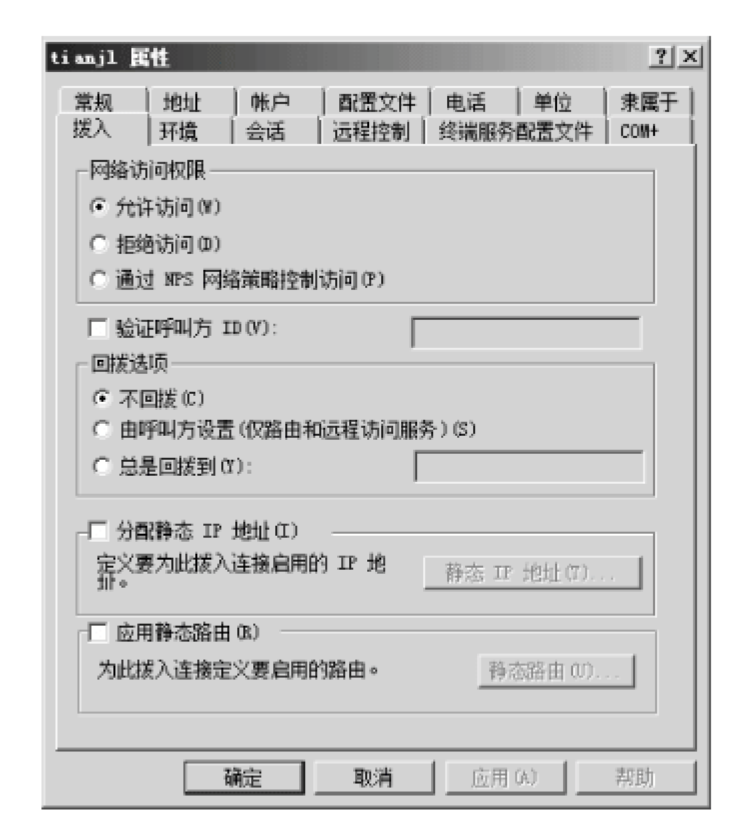


图 10-7　“tianjl 属性”对话框

5. 配置拨入用户账户

在 Active Directory 中，创建用于远程用户连接 VPN 服务器的用户组，并将远程分支机构用户对应的用户账户添加到组中。双击远程访问的用户账户（以 tianjl 用户账户为例），显示如图 10-7 所示的“tianjl 属性”对话框。在“网络访问权限”选项区域，选中“允许访

问"单选按钮,其他选项保持默认设置,单击"确定"按钮,保存设置即可。

10.2.2 安装和配置 VPN 服务器

VPN 服务器用来提供拨入功能,供远程计算机用户拨入公司局域网。不过,VPN 服务可以与网络策略服务器配合使用,对拨入的客户端用户进行验证,只允许通过网络安全验证的计算机才允许访问网络。VPN 服务器上需要安装两块网卡,一块网卡设置内网地址,用来连接局域网;另一块设置公网地址,用来连接 Internet。另外,如果希望使用 L2TP/IPSec 或 SSTP 安全连接,还必须为 VPN 服务器安装计算机证书。

1. 安装远程访问服务

(1) 单击"添加角色向导"链接,在"选择服务器角色"对话框中,选中"网络策略和访问服务"复选框,如图 10-8 所示。



图 10-8 "选择服务器角色"对话框

(2) 单击"下一步"按钮,显示"网络策略和访问服务"对话框,显示了网络策略和访问服务的简介信息。单击"下一步"按钮,显示如图 10-9 所示的"选择角色服务"对话框。由于只配置 VPN 服务器,因此,选中"路由和远程访问服务"复选框即可。

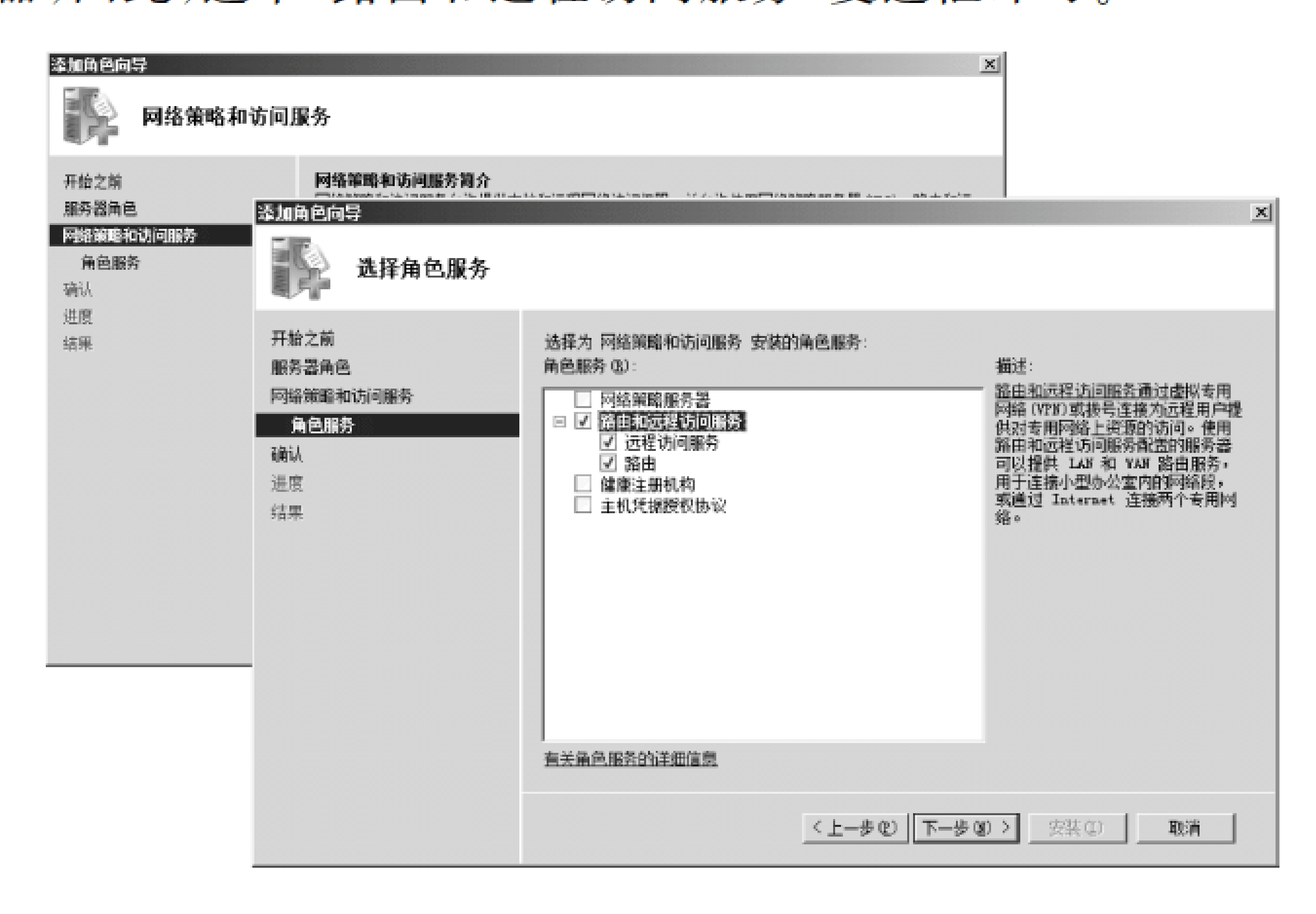


图 10-9 "选择角色服务"对话框

（3）单击“下一步”按钮，显示“确认安装选择”对话框，显示了将要安装的角色。单击“安装”按钮开始安装。完成后显示如图 10-10 所示的“安装结果”对话框。



图 10-10　“安装结果”对话框

（4）单击“关闭”按钮，远程访问服务安装完成。

2. 配置路由和远程访问服务

远程访问服务安装完成后，默认并没有启动，需要启用路由和远程访问功能。同时，由于 VPN 强制需要将远程拨入的用户向 NPS 服务器进行身份验证，以检查远程计算机是否符合策略要求，因此，还必须配置 RADIUS 服务器。

（1）依次选择“开始”→“管理工具”→“路由和远程访问”选项，打开“路由和远程访问”控制台窗口，如图 10-11 所示，默认没有启用路由和远程访问功能。

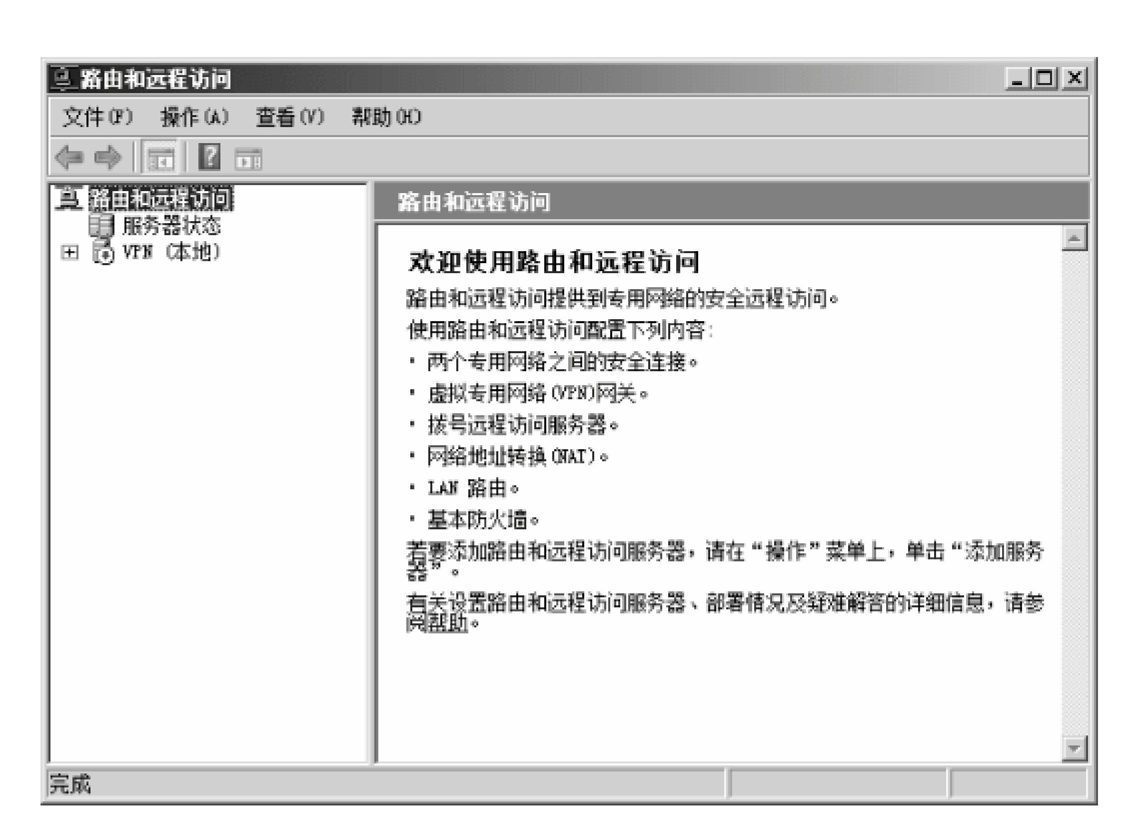


图 10-11　“路由和远程访问”控制台窗口

（2）右击服务器名并选择快捷菜单中的“配置并启用路由和远程访问”选项，启动“路由和远程访问服务器安装向导”。依次单击“下一步”按钮，设置远程访问方法和类型，如图 10-12 所示。



图 10-12　配置远程访问方法和类型

（3）依次单击“下一步”按钮，显示如图 10-13 所示的“VPN 连接”对话框，设置 VPN 远程访问服务器的网络连接。配置 VPN 远程访问服务器至少提供两块网卡，即一块连接 Internet，响应远程用户的访问；另一块用于连接内网。在“网络接口”列表中选择连接到 Internet 的接口即可。

（4）单击“下一步”按钮，管理员可以指定远程客户端获得 IP 地址的方式，如果本地网络中已经配置 DHCP 服务器，则可以选择“自动”方式，客户端可以从 DHCP 服务器获得内网 IP 地址。否则，可以选中“来自一个指定的地址范围”单选按钮，如图 10-14 所示。

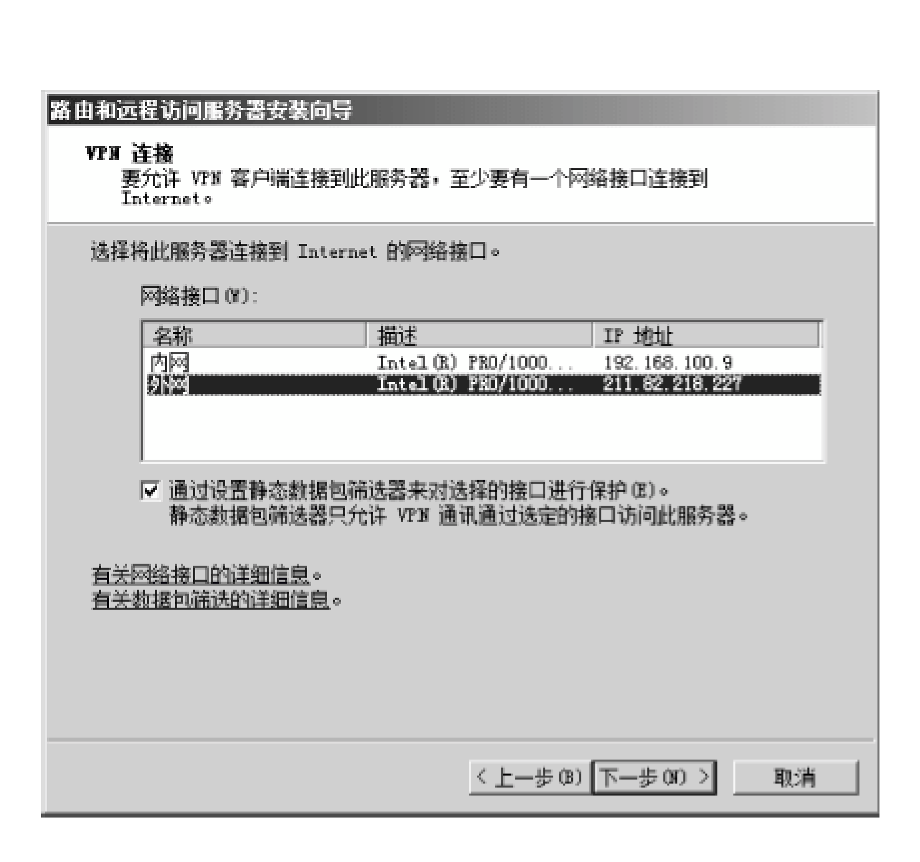


图 10-13　“VPN 连接”对话框

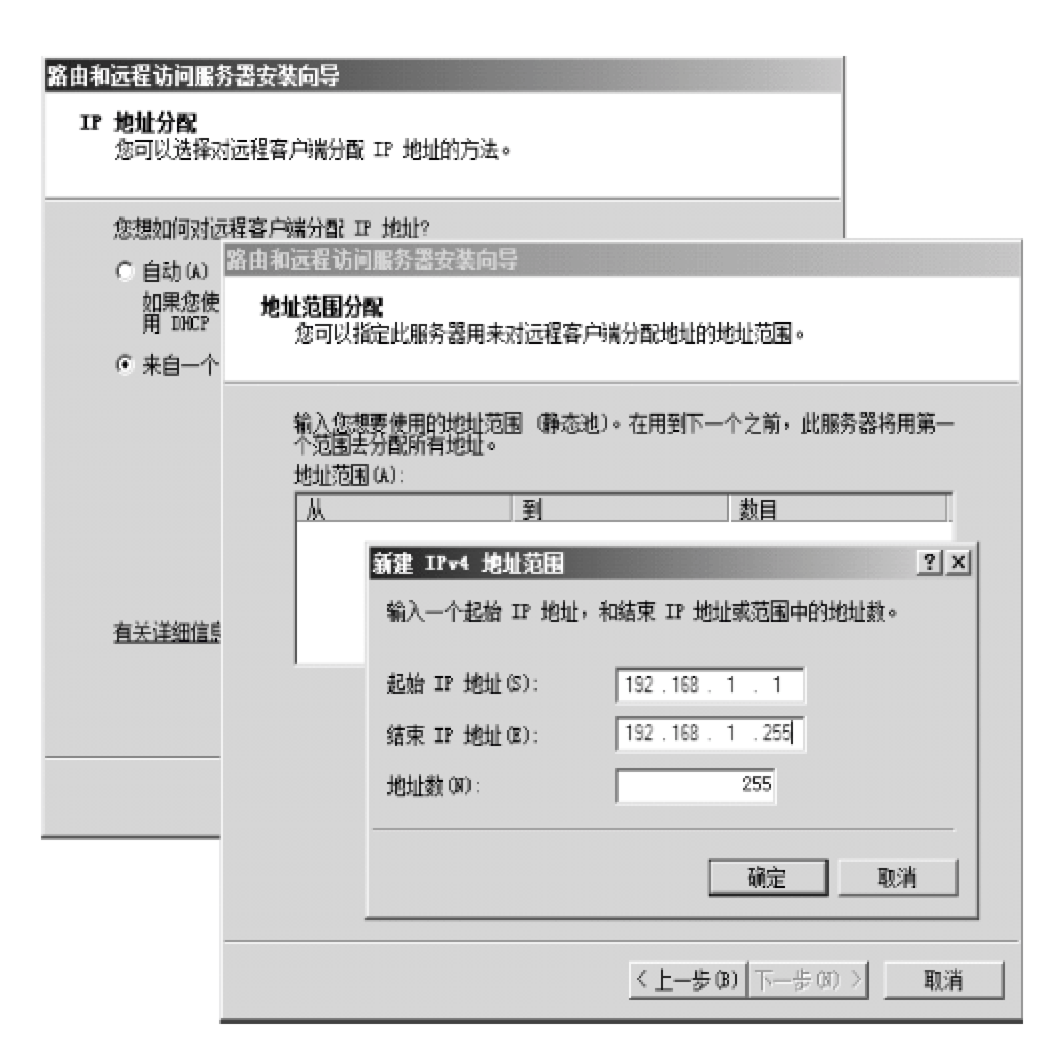


图 10-14　VPN 连接 IP 地址分配

（5）单击“下一步”按钮，显示“管理多个远程访问服务器”对话框。如果计划在专用网络上安装多个 VPN 服务器、无线访问点或其他 RADIUS 客户端，则添加 RADIUS 服务器非常有用，本例中选中“是，设置此服务器与 RADIUS 服务器一起工作”单选按钮。单击“下一步”按钮，显示“RADIUS 服务器选择”对话框，输入主、辅 RADIUS 的配置信息即可，如

图 10-15 所示。

(6) 单击“下一步”按钮，即可完成 VPN 服务器配置，此时会提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址，如图 10-16 所示。

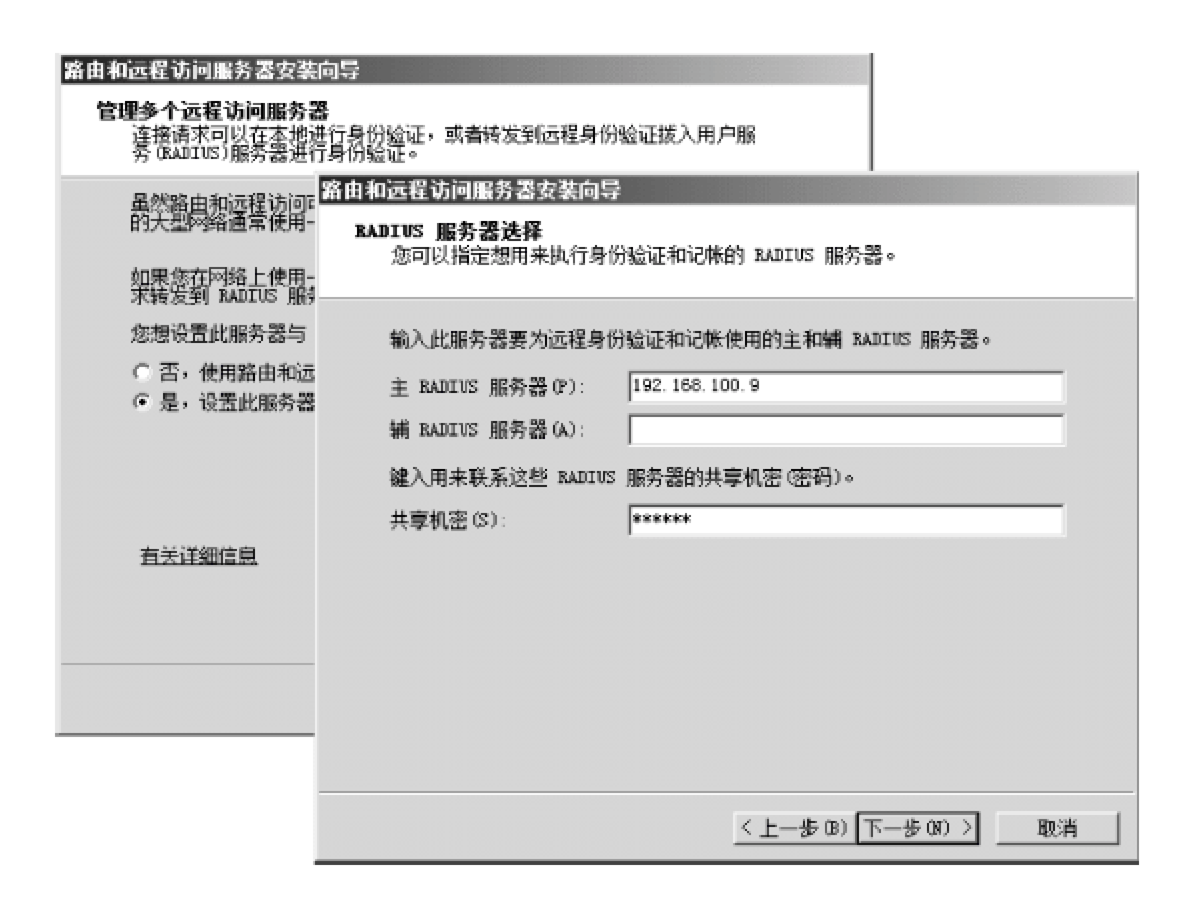


图 10-15 设置 RADIUS 身份验证选项

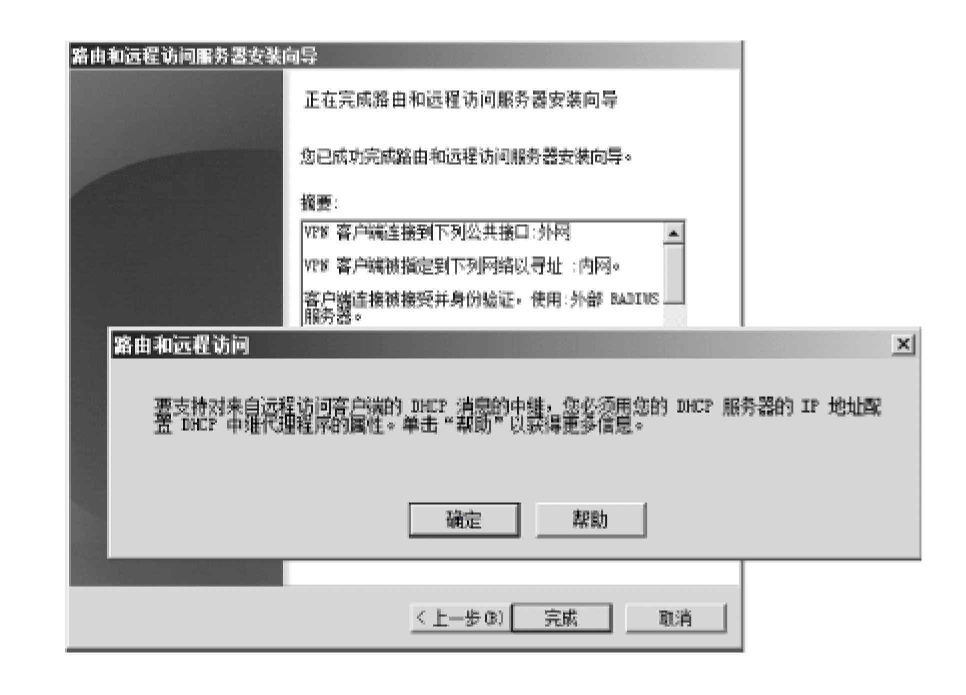


图 10-16 完成 VPN 远程访问服务器的配置

(7) 连续单击“确定”和“完成”按钮，即可完成 VPN 服务器的配置，显示如图 10-17 所示的配置结果。

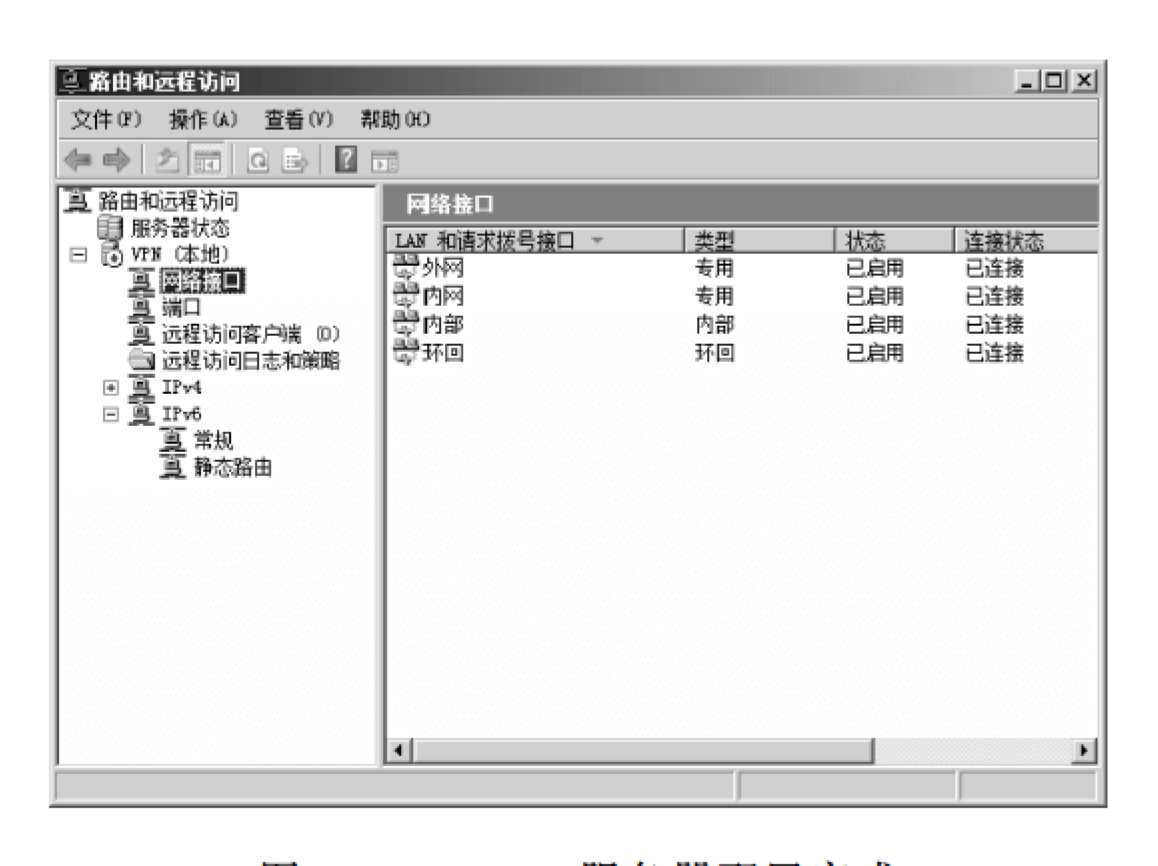


图 10-17 VPN 服务器配置完成

3. 配置静态路由和 RIP 路由

VPN 远程连接目的是以安全方式访问内网资源，仅建立 VPN 客户端到 VPN 服务器的连接是不够的。管理员必须为远程拨入用户设置路由信息，以确保其可以访问内网服务器或网络设备。为了使 VPN 服务器能够在内网中正确访问，管理员必须完成如下工作之一。

① 添加内网使用的 IPv4 和 IPv6 地址空间的静态路由。本例中使用 IPv4 协议。

② 如果用户在内网使用 RIP IPv4 路由连接 VPN 服务器，现有添加 RIP 路由协议，保证 VPN 服务器可以与临近的 RIP 路由器交换路由，并且为内网子网自动添加路由到路由表中。

配置静态路由和 RIP 路由的步骤如下。

(1) 打开“路由和远程访问”窗口,在左侧的窗格中选择 IPv4 节点,右击“静态路由”,在弹出的快捷菜单中选择“新建静态路由”选项,显示如图 10-18 所示的“IPv4 静态路由”对话框,为静态路由选择适当的“接口”、“目标”、“网络掩码”、“网关”和“跃点数”。单击“确定”按钮,即可创建到内网的静态路由。



图 10-18 添加 IPv4 静态路由

(2) 在“路由和远程访问”窗口左侧窗格中选择 IPv4 节点。右击“常规”,在弹出的快捷菜单中选择“新建路由协议”选项,显示如图 10-19 所示的“新路由协议”对话框,选中“用于 Internet 协议的 RIP 版本 2”路由协议。

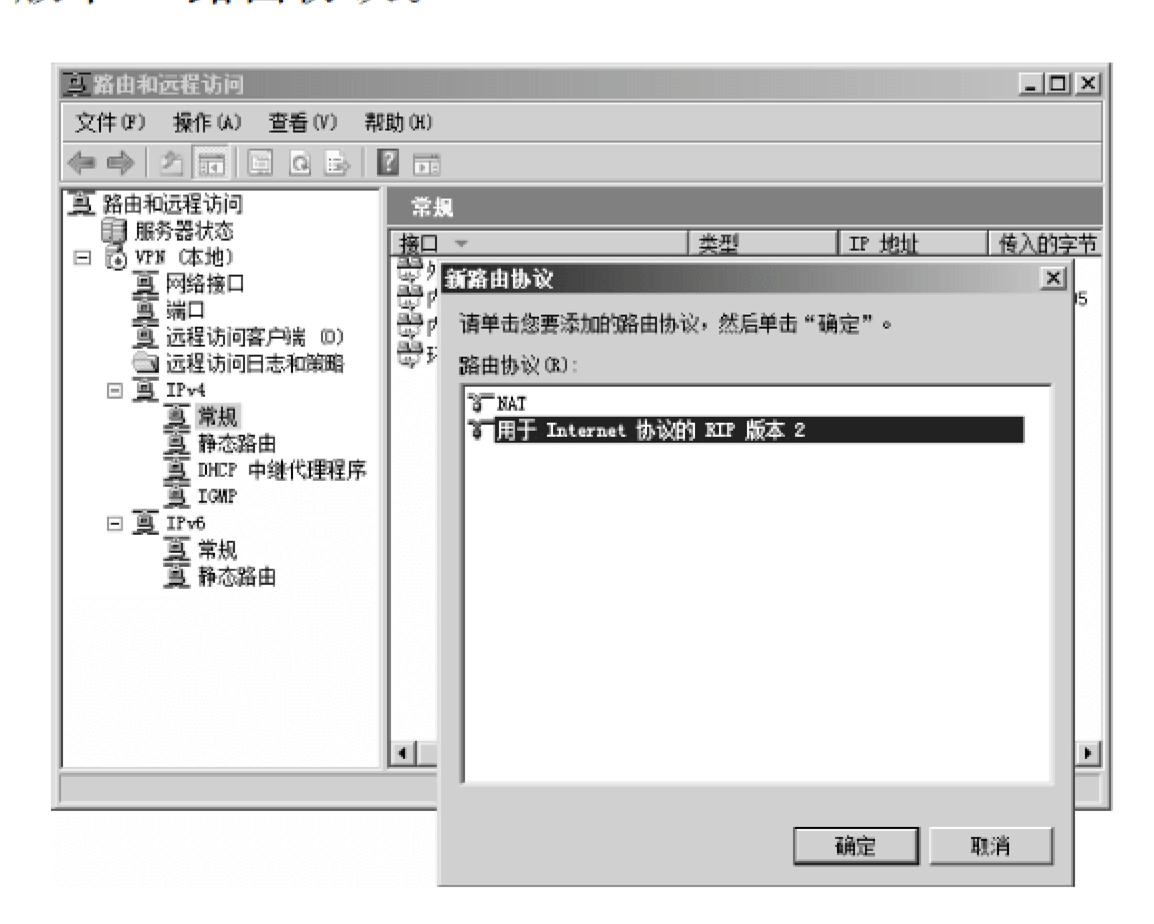


图 10-19 将 VPN 服务器配置为 RIP 路由器

(3) 单击“确定”按钮返回“路由和远程访问”对话框。右击 RIP,在弹出的快捷菜单中选择“新增接口”选项,显示如图 10-20 所示的“用于 Internet 协议的 RIP 版本 2 的新接口”对话框,选择 VPN 服务器内网网卡即可。

(4) 单击“确定”按钮,显示如图 10-21 所示的“RIP 属性 - 外网 属性”对话框,根据现有配置 RIP 路由协议参数,建议使用默认值即可。

(5) 单击“确定”按钮,完成 RIP 路由协议的配置。



图 10-20 “用于 Internet 协议的 RIP 版本 2 的新接口”对话框



图 10-21 “RIP 属性 - 外网 属性”对话框

4. 部署“自动证书申请设置”策略

SSL VPN 和 IPSec VPN 的客户端访问服务器时都要用到证书进行身份验证。总部网络中部署的企业根证书服务器支持加入域的计算机自动申请证书，通过“自动证书申请设置”策略为域中的计算机自动颁发证书。

(1) 以域管理员身份登录到域控制器，选择“开始”→“管理工具”→“组策略管理”选项，打开如图 10-22 所示的“组策略管理”窗口。依次展开“组策略管理”→“林：coolpen.net”→“域”→coolpen.net→Default Domain Policy 策略。

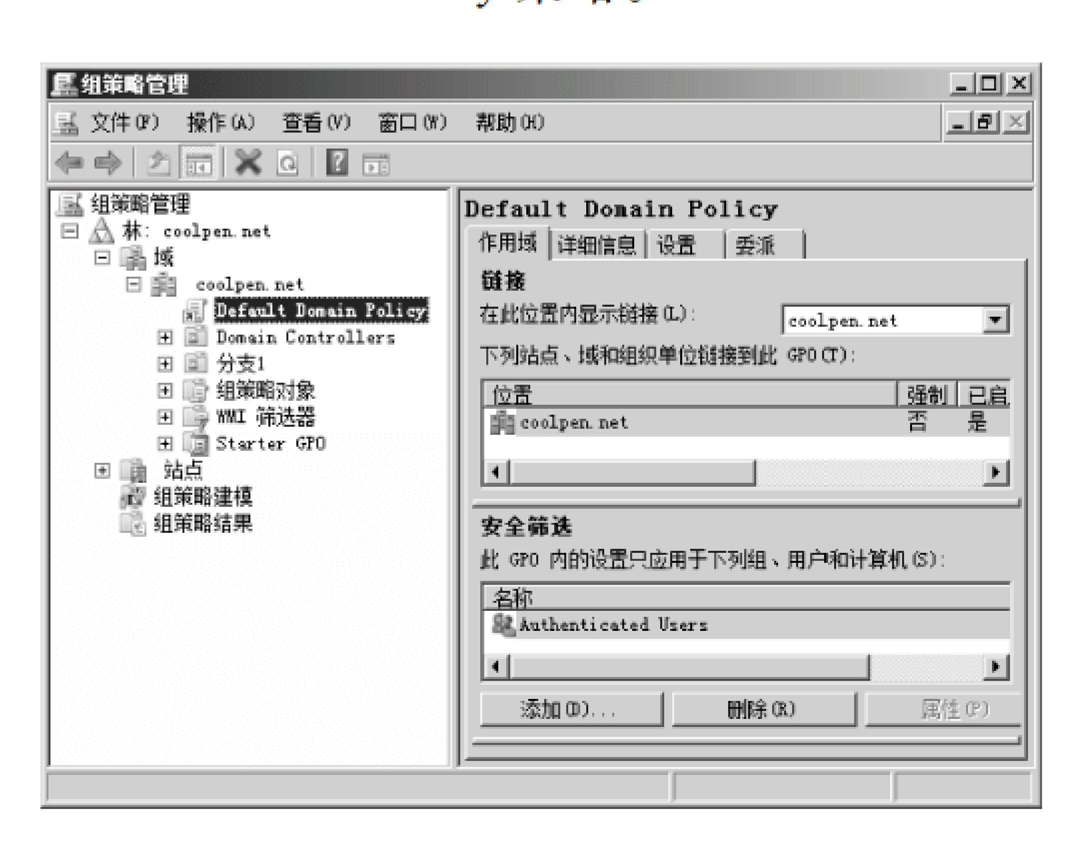


图 10-22 “组策略管理”窗口

(2) 右击 Default Domain Policy 策略选择快捷菜单中的“编辑”选项，显示如图 10-23 所示的“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“公钥策略”→“自动证书申请设置”选项，右击“自动证书申请设置”选项，在弹出的快捷菜单中选择“新建”→“自动证书申请”选项，启动“自动证书申请设置向导”。

(3) 单击“下一步”按钮，显示如图 10-24 所示的“证书模板”对话框。在“证书模板”列表中选择“计算机”模板。

(4) 单击“下一步”按钮，显示如图 10-25 所示的“正在完成自动证书申请设置向导”对话框。单击“完成”按钮，成功创建新的策略。

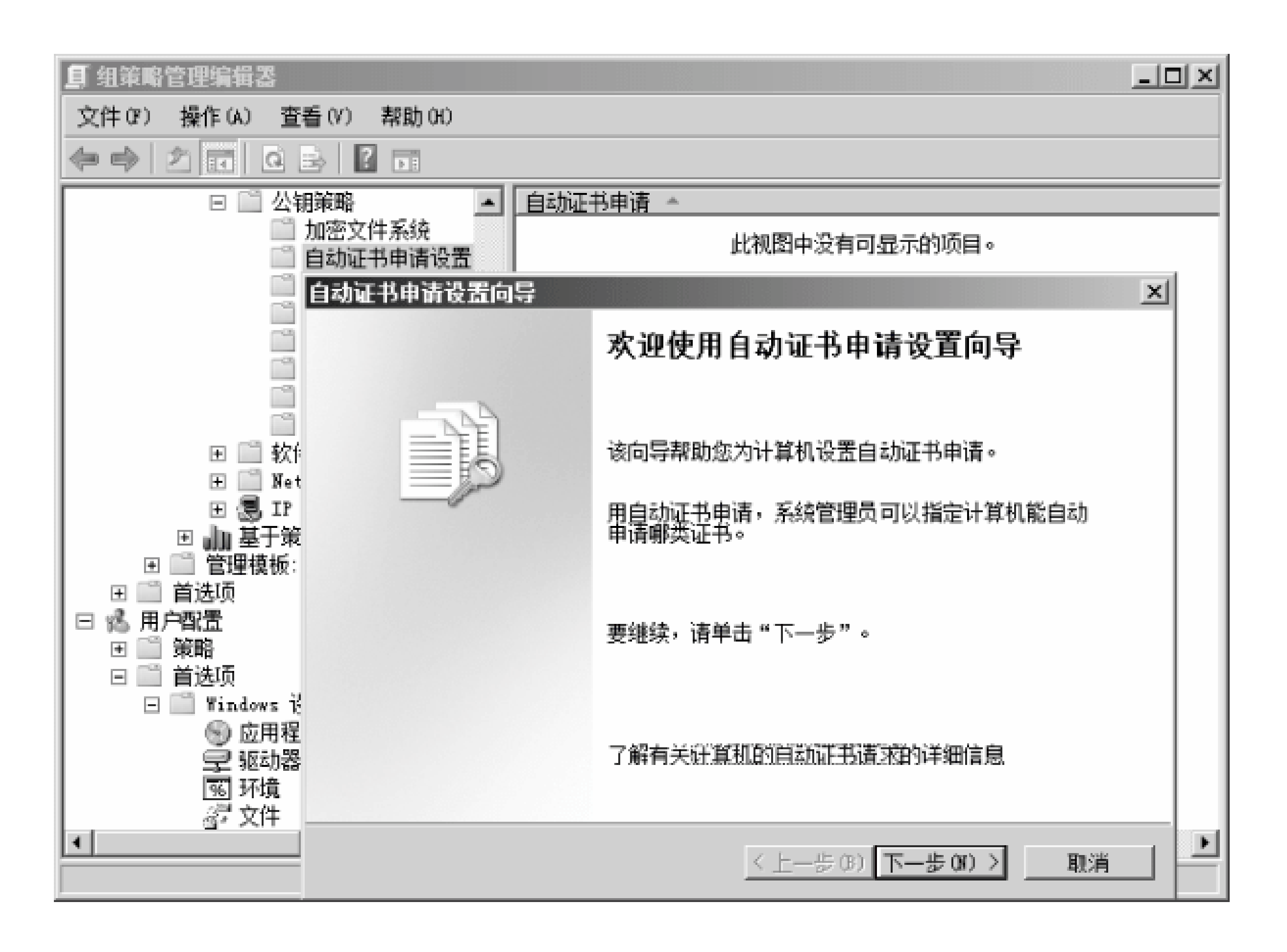


图 10-23 “组策略管理编辑器”窗口

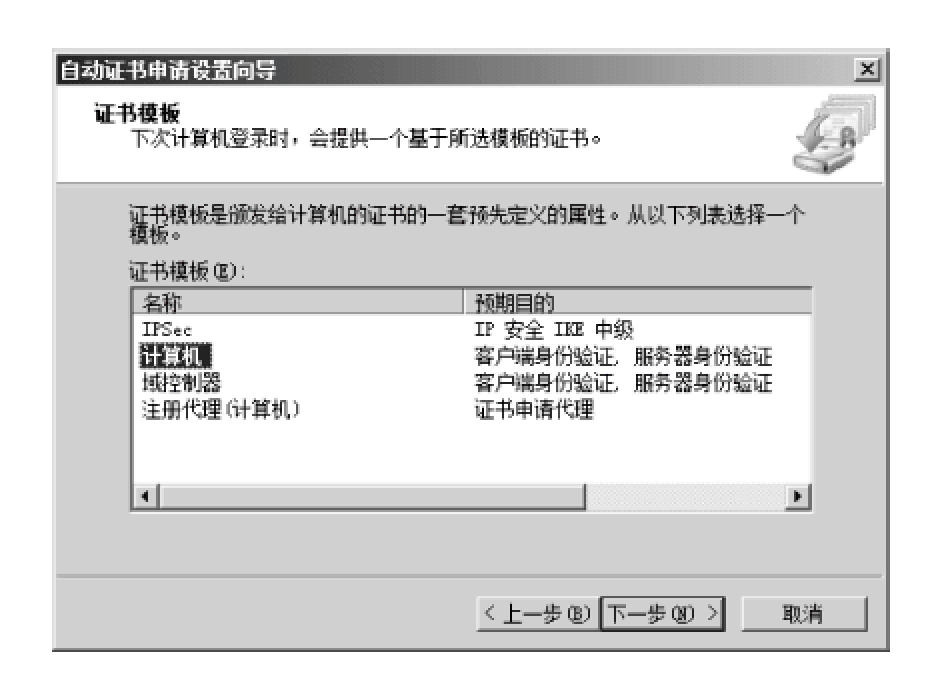


图 10-24 “证书模板”对话框

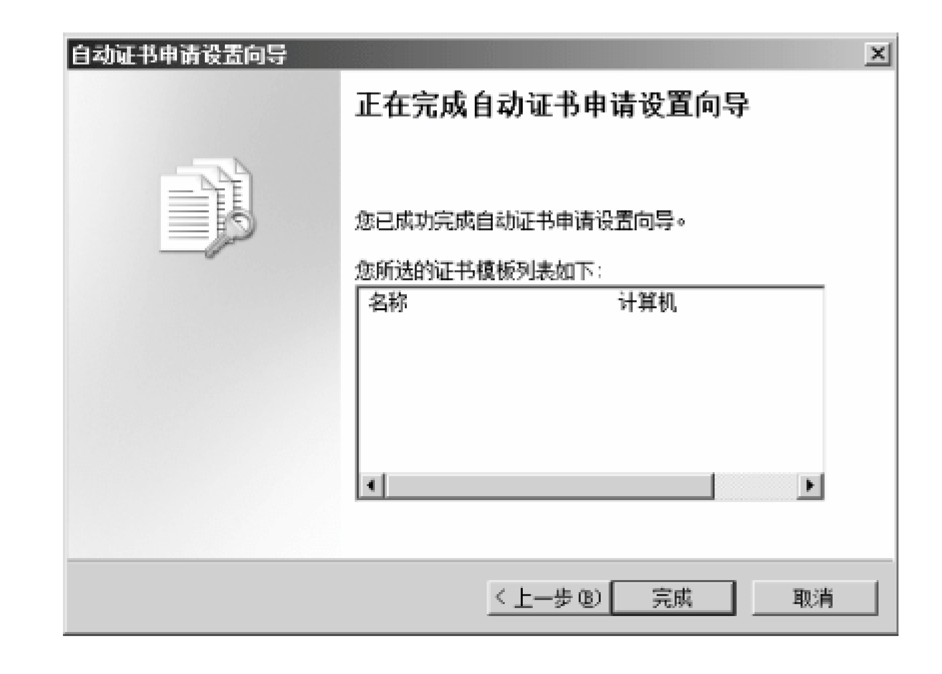


图 10-25 “正在完成自动证书申请设置向导”对话框

10.2.3 配置 SSL VPN

SSL VPN 技术是 VPN 安全技术的主要发展方向，大多数 VPN 设备以及 Windows Server 2008 和 Windows Vista SP1 都支持该技术。SSL VPN 技术主要应用于远程访问 VPN，并且支持 Web 方式的 VPN 连接。

1. 验证 VPN 服务器的计算机证书

部署 SSL VPN 服务器需要从 Active Directory 证书服务器中得到证书，如果没有配置证书，SSL VPN 客户端计算机将不能连接到 SSL VPN 服务器。SSL VPN 服务器使用的证书可以通过部署的域组策略自动完成申请以及注册。

(1) 以管理员账户登录 VPN 服务器，新建一个控制台窗口，单击“文件”菜单，选择“添加或删除管理单元”选项，在“可用的管理单元”列表中选中“证书”并单击“添加”按钮，选中“计算机账户”单选按钮并单击“下一步”按钮，在“选择计算机”对话框中选中“本地计算机”单选按钮，单击“完成”按钮将其添加到“所选管理单元”列表中，如图 10-26 所示。

(2) 在“证书”管理控制台中，依次展开“证书(本地计算机)”→“个人”→“证书”选项，检查是否已经自动注册了计算机证书，双击证书名称即可查看证书的详细信息，如图 10-27 所示。



图 10-26　添加“证书”管理单元



图 10-27　检查 VPN 服务器的计算机证书

提示：如果 VPN 服务器没有自动注册到计算机证书，则需要手动为其向企业根 CA 申请计算机证书。

2. 创建 SSL VPN 客户端

只有运行 Windows Vista 操作系统和 Windows Server 2008 操作系统的计算机才支持 SSL VPN 客户端，Windows XP/2000/2003 操作系统不支持 SSL VPN 客户端。

(1) 打开“网络和共享中心”窗口，单击“设置连接或网络”链接，打开“选择一个连接选项”对话框，选择“连接到工作区”选项。单击“下一步”按钮，既可以选择通过 Internet 连接建立 VPN 连接，也可以选择直接拨号方式建立 VPN 连接。单击“使用我的 Internet 连接(VPN)”选项，显示“键入要连接的 Internet 地址”对话框，在“Internet 地址”文本框中输入 VPN 服务器的域名或公网 IP 地址，既可以是 IPv4 地址，也可以是 IPv6 地址。在“目标名称”文本框中输入进行 VPN 连接时显示的名称，如图 10-28 所示。

提示：为了确保此拨号连接的安全，可以设置相应的安全措施。



图 10-28　设置连接方式和 VPN 服务器信息

① 使用智能卡。智能卡是包含用户账户重要信息的芯片,使用时需将个人专用智能卡插入计算机的读卡器,如果提供的身份信息通过系统验证,则可以使用该连接,否则将无法应用。使用智能卡比使用密码更能提高安全级别,但实现成本也较高。

② 允许其他人使用此连接。允许当前计算机上的任何用户账户使用此连接,登录到 VPN 服务器。

(2) 单击"下一步"按钮,分别在"用户名"和"密码"文本框中,输入 VPN 服务器上指派的用于 VPN 拨叫的用户账户和密码即可。单击"连接"按钮,即可尝试连接到远程 VPN 服务器,如图 10-29 所示。成功连接后,即可像在同一局域网中一样,使用 VPN 服务器连接的子网中的各种资源。

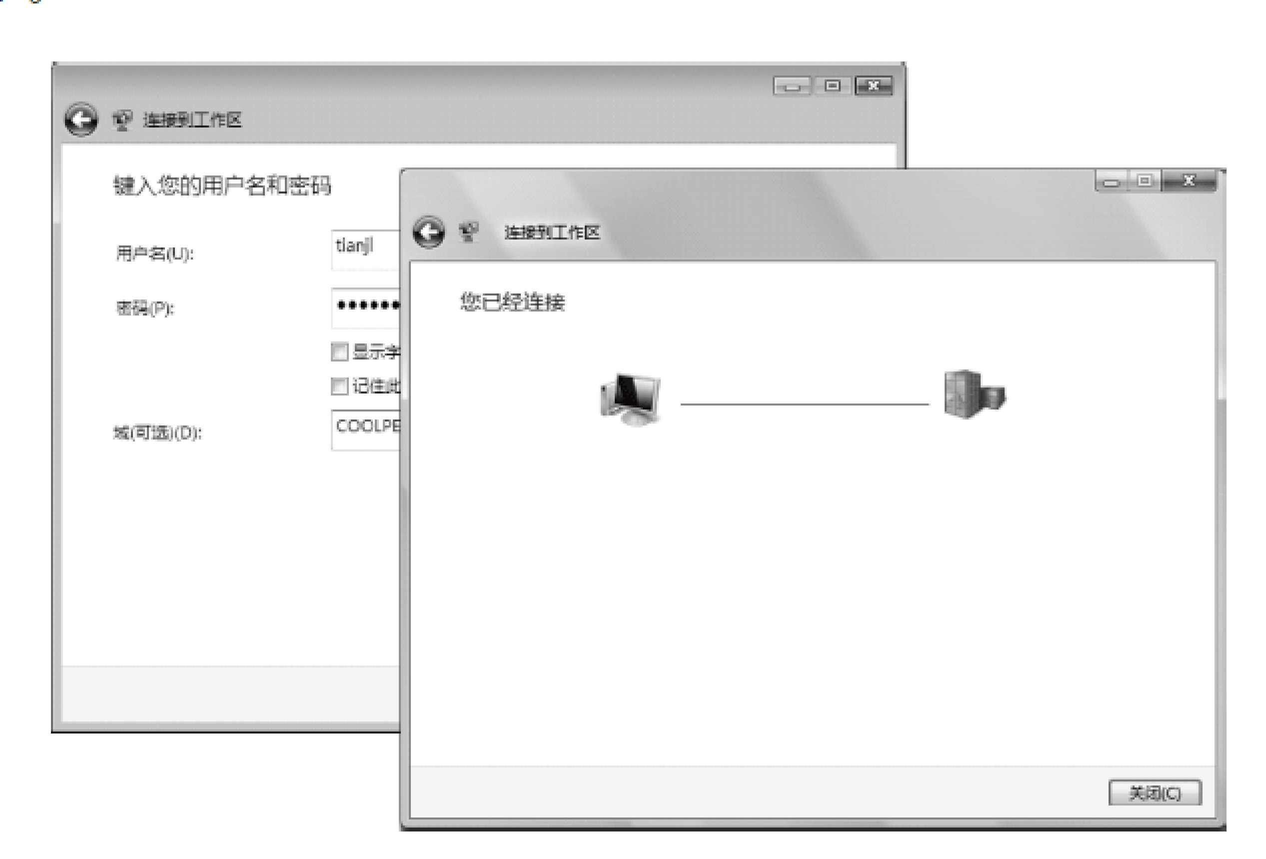


图 10-29　设置身份验证信息并尝试连接

如果以后需要使用 VPN 连接远程网络时,可在"网络和共享中心"中单击"管理网络连接"链接,在"网络连接"窗口中双击所创建的 VPN 连接,显示如图 10-30 所示的"连接 VPN 连接"对话框,单击"连接"按钮即可连接。而右击 VPN 连接并选择快捷菜单中的"断开"选

项，则可断开 VPN 连接。

（3）打开“网络连接”窗口。右击已创建的 VPN 连接，在弹出的快捷菜单中选择“属性”选项，显示如图 10-31 所示的“VPN 连接 属性”对话框。切换到“网络”选项卡，在“VPN 类型”下拉列表框中，选择“安全套接字隧道协议（SSTP）”选项，当 VPN 客户端计算机证书设置成功后，即可登录 SSL VPN 服务器。



图 10-30　连接 VPN 连接

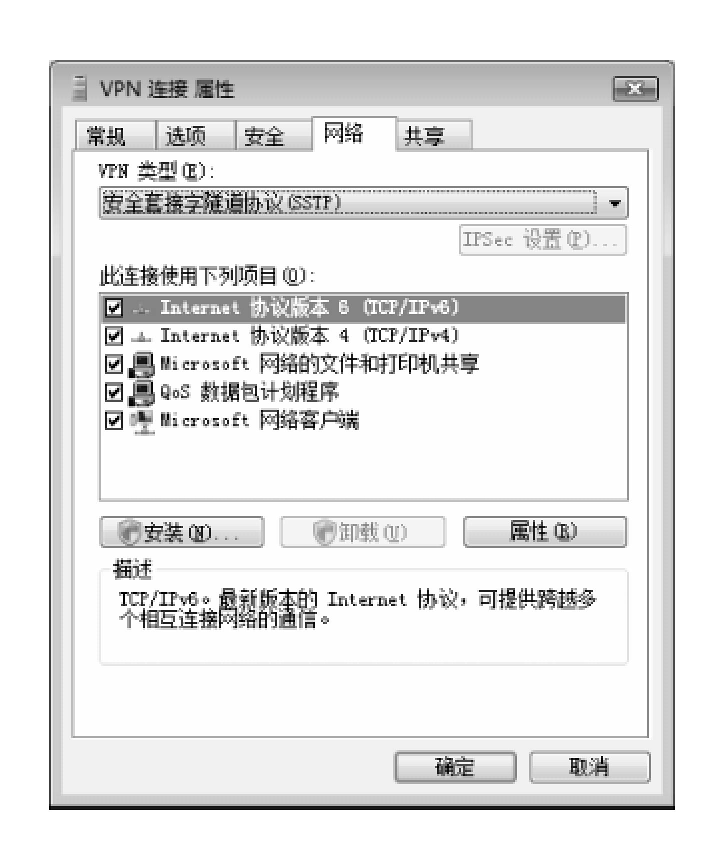


图 10-31　“VPN 连接 属性”对话框

3. 配置 VPN 客户端证书信任

VPN 客户端登录 VPN 服务器之前必须先通过证书身份验证，即必须建立客户端与 VPN 服务器所在网络的证书服务器的证书信任。

（1）以域用户身份通过 SSL VPN 客户端模式连接到内部网络中，打开 Internet Explorer 浏览器，在地址栏中输入“http://企业根证书服务器/certsrv”并按 Enter 键，打开证书服务 Web 窗口。单击“下载 CA 证书、证书链或 CRL”链接，显示如图 10-32 所示的窗口。



图 10-32　证书服务 Web 窗口

(2) 单击“下载 CA 证书”链接，显示如图 10-33 所示的“文件下载-安全警告”对话框，可以直接打开，也可以单击“保存”按钮，暂时保存在本地计算机。

(3) 单击“打开”按钮，显示如图 10-34 所示的“证书”对话框，在“常规”选项卡中单击“安装证书”按钮，启动“证书导入向导”。



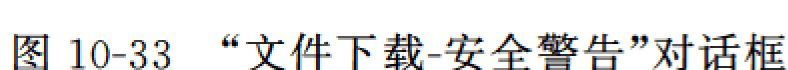

图 10-33 “文件下载-安全警告”对话框



图 10-34 “证书”对话框

(4) 单击“下一步”按钮，显示如图 10-35 所示的“证书存储”对话框，选中“将所有的证书放入下列存储”单选按钮，单击“浏览”按钮，在“选择证书存储”对话框中选择“受信任的根证书颁发机构”并单击“确定”按钮。

(5) 单击“下一步”按钮，显示“正在完成证书导入向导”对话框。单击“完成”按钮，关闭“证书导入向导”，显示如图 10-36 所示的“安全性警告”对话框。单击“是”按钮，提示证书导入成功。

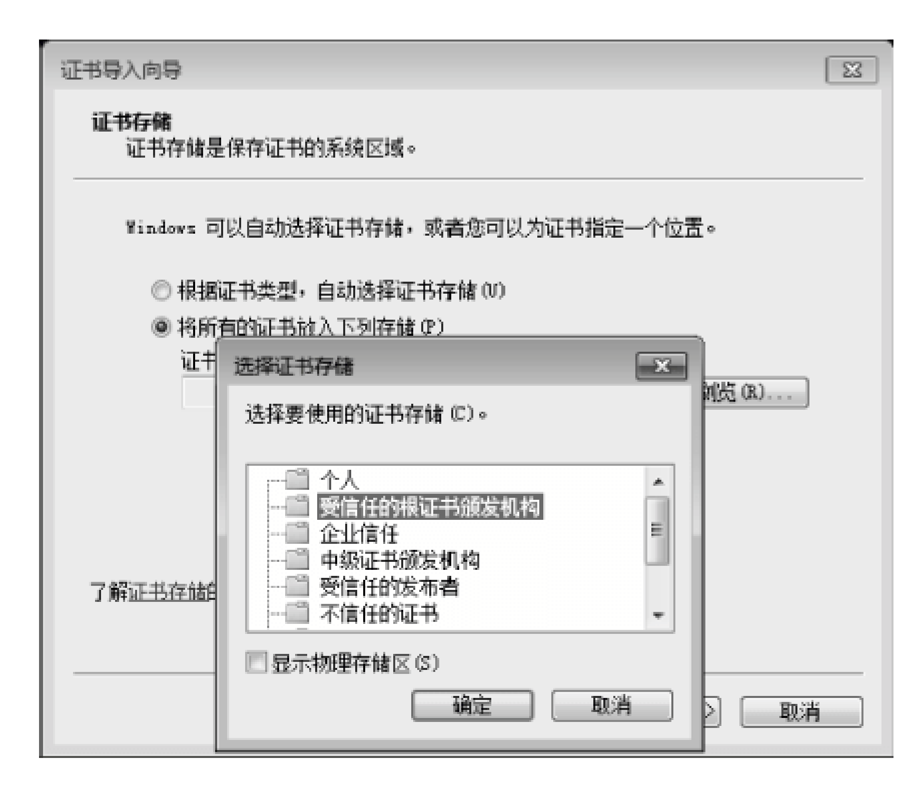


图 10-35 “证书存储”对话框

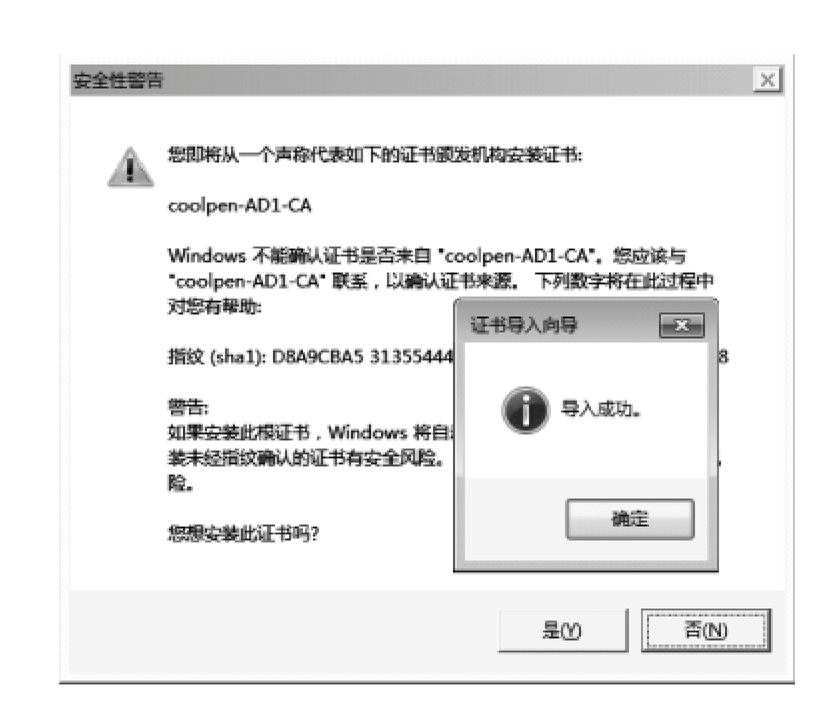


图 10-36 “安全性警告”对话框

4. VPN 客户端连接

(1) 打开“网络连接”窗口，右击已创建的 VPN 连接，在弹出的快捷菜单中选择“连接”命令，显示“连接到 VPN 连接”对话框。由于在设置过程中，已经输入登录 SSL VPN 服务器用户名和密码，在该对话框中自动输入用户名、密码以及目标域。单击“连接”按钮，即可开始连接，成功连接后“VPN 连接”的状态会显示为“已连接”，如图 10-37 所示。

(2) 右击已连接的“VPN 连接”，在弹出的快捷菜单中选择“状态”选项，显示如



图 10-37　SSL VPN 客户端连接

图 10-38 所示的“VPN 连接 状态”对话框。

(3) 切换到“详细信息”选项卡，显示如图 10-39 所示的“详细信息”选项卡。列表中的“设备名”值表示远程客户端计算机通过 SSL 模式连接到 SSL VPN 服务器。



图 10-38　“VPN 连接 状态”对话框



图 10-39　“详细信息”选项卡

10.2.4　配置 IPSec VPN

与 SSL VPN 相比，IPSec VPN 技术更早一些，对客户端系统要求也相对较低。Windows XP/2003/Vista/2008 都可以配置为 IPSec VPN 客户端。IPSec VPN 主要应用于远程网络互联 VPN，即点对点 VPN，当然也可以用于部署远程访问 VPN。此处仍以配置远程访问 IPSec VPN 为例介绍主要实现过程。管理员可以通过共享密钥和证书两种方式部署 IPSec VPN。

1. 共享密钥配置 IPSec VPN

通过预先指定 IPSec VPN 双方使用的身份验证密钥(共享密钥)，可以快速建立 VPN 通信。需要注意的是，由于采用预先共享密钥的验证方式，其安全性比采用凭证验证的方式来得差，因此只建议使用在测试环境，不建议使用在正式环境中。IPSec VPN 服务器的搭建和配置过程与前面介绍的 SSL VPN 大致相同，这里只介绍不同之处。

（1）VPN 服务器的配置

在 VPN 服务器上打开“路由和远程访问”窗口，右击 VPN 服务器名称并选择快捷菜单中的“属性”选项，显示如图 10-40 所示的“VPN（本地）属性”对话框，在“安全”选项卡中选中“允许 L2TP 连接使用自定义 IPsec 策略”复选框，并在“预共享的密钥”文本框中输入一个自定义密钥，例如 123456。客户端需要设置与 VPN 服务器完全相同的共享密钥，否则无法建立连接。

单击“确定”按钮，保存设置。此时系统会提示重新启动“路由和远程访问”服务后更改才会生效，按照提示重启服务即可。



图 10-40 “VPN（本地）属性”对话框



图 10-41 “IPsec 设置”对话框

（2）VPN 客户端的配置

登录到 VPN 客户端计算机，右击创建好的 VPN 拨号连接，选择快捷菜单中的“属性”选项，打开“VPN 连接 属性”窗口，切换到“网络”选项卡，在“VPN 类型”下拉列表框中选择 L2TP IPsec VPN 选项，单击“IPSec 设置”按钮，显示如图 10-41 所示的“IPsec 设置”对话框，选中“使用预共享的密钥作身份验证”单选按钮，并在“密钥”文本框中输入与服务器端完全相同的密钥。最后，连续单击“确定”按钮，保存设置。

（3）测试配置结果

在 VPN 客户端计算机上，双击 VPN 拨号连接，使用预先设定的用户名和密码拨叫到 VPN 服务器上。右击已成功连接的 VPN 连接，选择快捷菜单中的“状态”选项，显示如图 10-42 所示的“VPN 连接 状态”对话框，在“详细信息”选项卡的“设备名”中可以看到此时使用的协议是 L2TP。

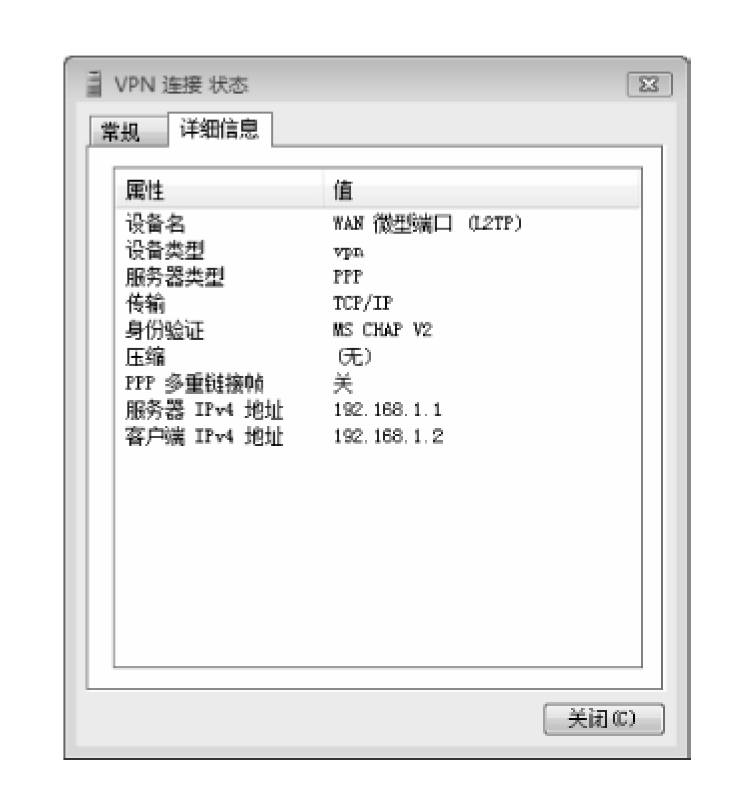


图 10-42 “VPN 连接 状态”对话框

2．使用证书配置 IPSec VPN 连接

使用数字证书作为 IPSec VPN 通信双方身份验证的方式，显然比预共享密钥更加安全，因此在实现机制上也稍显复杂一些，与 SSL VPN 一样，需要用到证书服务器。接下来的测试工作仍然基于配置 SSL VPN

之前的基础环境。

（1）服务器端的配置

由于在先前的准备工作中已经部署了“自动证书申请设置”策略，证书服务器可以自动为 VPN 服务器和 VPN 客户端分配计算机证书，因此也就无须一一为服务器和客户端注册计算机证书。不过，还需要建立 VPN 服务器和 CA 之间的证书信任，即下载证书服务器的 CA 证书或证书链，并将其导入到 VPN 服务器“受信任的根证书颁发机构”中，如图 10-43 所示。



图 10-43　建立 VPN 服务器到 CA 的证书信任关系

（2）客户端的配置

与 VPN 服务器端相同，IPSec VPN 客户端也需要申请计算机证书和配置证书信任（如图 10-44 所示），操作方法此处不再赘述。

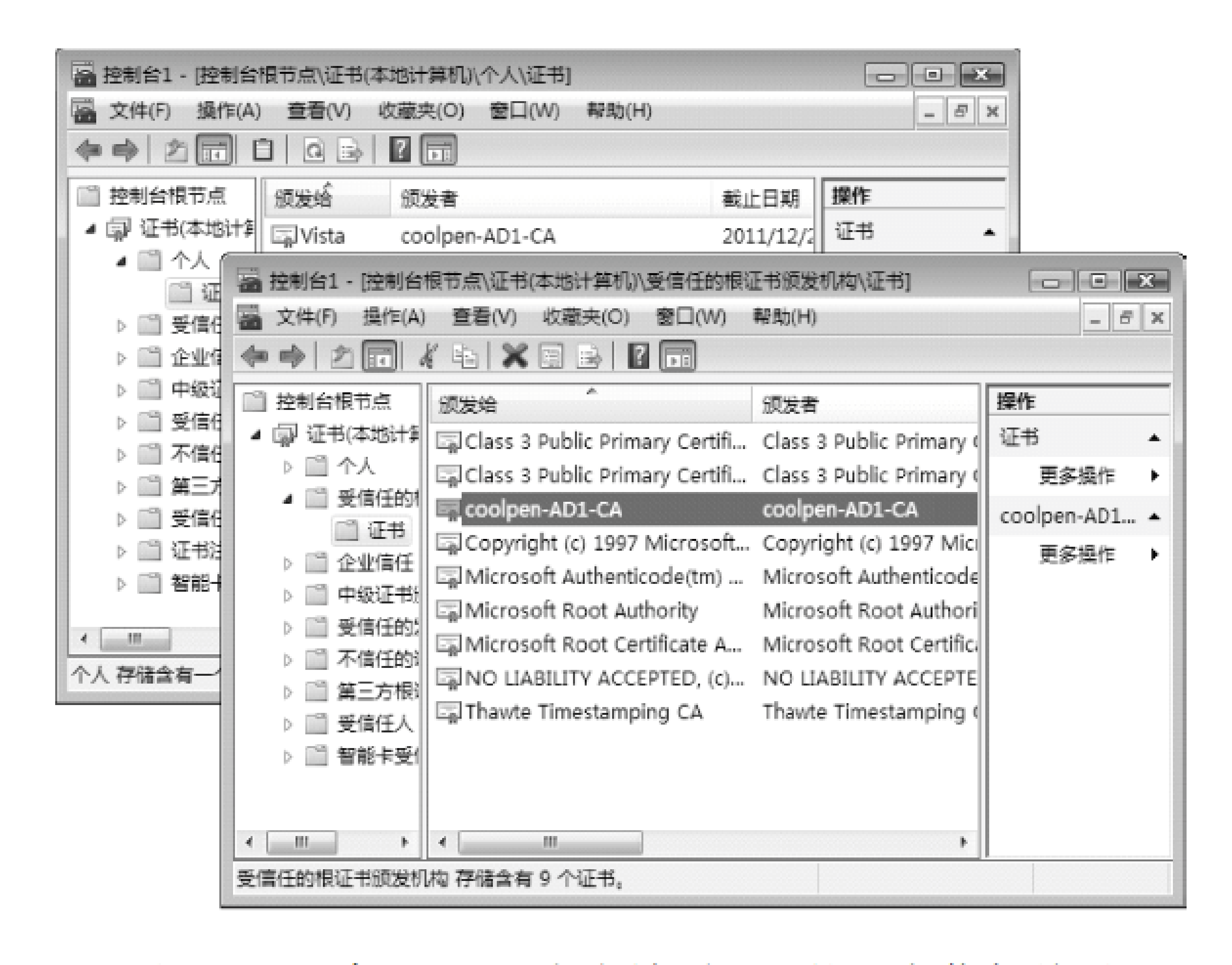


图 10-44　建立 VPN 客户端到 CA 的证书信任关系

IPSec VPN 客户端连接的与 SSL VPN 客户端类似，只是需要在连接之前进行一些必要的连接模式更改。仍然以 Windows Vista 客户端为例，右击创建好的 VPN 网络连接，选

择快捷菜单中的“属性”选项，打开如图 10-45 所示的“VPN 连接 属性”对话框，切换到“网络”选项卡，在“VPN 类型”下拉列表框中选择 L2TP IPsec VPN 选项，单击“IPsec 设置”按钮，显示“IPsec 设置”对话框，选中“将证书用于身份验证”单选按钮，并选中“验证服务器证书的 Name 和 Usage 属性”复选框。



图 10-45 “VPN 连接 属性”对话框

(3) 测试配置结果

VPN 客户端成功连接到 VPN 服务器后，双击 VPN 网络连接，即可查看其详细状态信息，与使用共享密钥方式建立 IPSec VPN 连接客户端相同，此处不再赘述。

10.2.5 知识链接：VPN 的应用类型、SSL VPN 和 IPSec VPN

1. VPN 的应用类型

VPN 本身就是一种为远程访问提供安全保障的技术，因此通常应用于连接异地局域网，并且实现安全通信。一般来说，VPN 适用于 3 种情况：通过 Internet 实现远程用户访问、通过 Internet 实现网络互联和连接内部网络计算机。

(1) 远程用户访问

VPN 允许用户安全地通过 Internet 远程访问企业资源，与使用专线拨打长途或电话连接企业的网络接入服务器(NAS)不同，VPN 用户首先拨通本地 ISP 的 NAS，然后 VPN 软件利用与本地 ISP 建立的连接，在拨号用户和 VPN 服务器之间创建一个跨越 Internet 或其他公共互联网络的虚拟专用网络。例如，用户想要在家中计算机上访问公司网络中的机密数据，首先家庭计算机向本地 ISP 发出请求，然后通过 Internet 拨叫到公司网络的 VPN 服务器，从而在两者之间创建一条虚拟通道，其工作模式如图 10-46 所示。

(2) 网络互联

使用 VPN 技术还可以建立异地局域网之间的安全连接。首先在每个局域网中配置一台 VPN 服务器，然后将其接入 Internet，并允许接收拨入请求和向对端发送连接请求，这样即可实现异地网络的安全互联(如图 10-47 所示)。

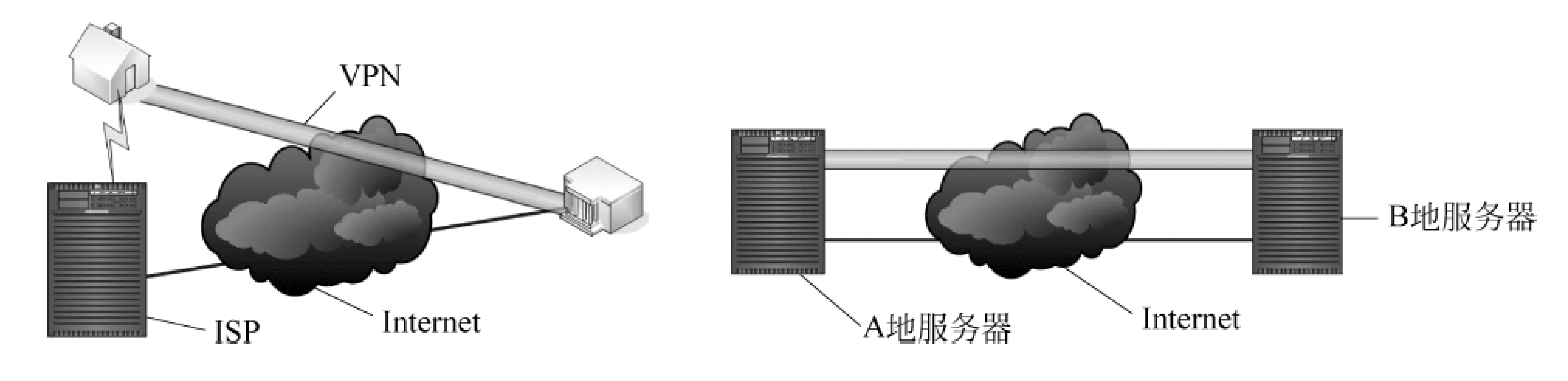


图 10-46 用户远程访问局域网　　图 10-47 使用专线连接异地局域网

(3) 连接内部网络计算机

在企业的内部网络中，某些部门可能存储有重要数据，为确保数据的安全性，传统的方

式只能是把这些部门同整个企业网络断开,形成孤立的小网络。这样做虽然保护了部门的重要信息,但是由于物理上的中断,造成其他部门的用户之间通信困难。

采用 VPN 方案时,通过一台 VPN 服务器既可实现与整个企业网络的连接,又能保证保密数据的安全性。而路由器虽然也能够实现网络之间的互联,但是并不能对流向敏感网络的数据进行限制。企业网络管理人员通过使用 VPN 服务器,指定只有符合特定身份要求的用户才能连接并获得访问敏感信息的权利。此外,可以对所有 VPN 数据进行加密,从而确保数据的安全性。

2. SSL VPN 和 IPSec VPN

SSL VPN 和 IPSec VPN 均支持远程访问 VPN,相比较而言 SSL VPN 具有部署简单,无客户端,维护成本低,网络适应强等特点。SSL VPN 和 IPSec VPN 技术的详细对比如表 10-1 所示。

表 10-1　SSL VPN 和 IPSec VPN 对比

比较项目	SSL VPN	IPSec VPN
VPN 网络类型	远程访问 VPN 为主	远程网络互联 VPN(必须使用 IPSec VPN)也支持远程访问 VPN
主要应用选择	Web 应用为主	CS 应用,甚至三层应用为主
	单项应用访问为主	双向应用访问
	不支持 VOIP 类协议	需要支持 VOIP 类协议
	无广播包类型应用	有广播包类型应用
用户类型	合作伙伴或者客户、内部用户、移动用户	内部用户
	使用无法控制的设备接入的用户	能明确使用手控的设备接入的移动用户
网络终端类型	计算机、掌上电脑、手机等,操作系统种类复杂	主要是计算机,操作系统类型单一,例如全部是 Windows
	无须维护客户端	需要专业的 IT 部门或设备供应商维护 VPN 终端

10.3　配置路由器 VPN

路由器是每个企业网络的必备设备之一。目前大多数路由器产品都已经集成 VPN 功能,它不同于提供专业 VPN 模块插槽的模块化路由器,无须增加任何投资即可获得高效可靠的 VPN 连接。但是,这类 VPN 网络的性能直接取决于路由器本身,高性能的路由器往往可以支持更多数量的 VPN 客户端,并且可靠性也较高。

并非所有的路由器产品都可以用来实现 VPN 连接,这取决于路由器硬件支持和 IOS 版本两个方面。

版本较早的路由器和宽带路由器本身就没有提供 VPN 功能,以 Cisco 路由器为例,Cisco 800 系列的宽带路由器中很少提供 VPN 支持,并且在后来的 Cisco 2600 系列产品中,部分产品也只能提供功能简单的 VPN 支持,尚无法支持许多高级别的加密算法。不仅如此,在当前许多新型的 Cisco 模块化路由器中,也取消了 VPN 支持,取而代之的是专用 VPN 模块插槽。

如果确认路由器硬件可以支持 VPN,则还要看运行的软件系统是否支持。仍以 Cisco 路由器为例,有些版本的 IOS 是不支持 VPN 功能的,即使路由器本身支持该功能,也无法顺利实现,必须升级或降级到相应版本的 IOS 才可以。

另外,借助路由器实现 VPN 时,必须使用防火墙作为 Internet 接入设备,此时的路由器只做 VPN 服务器,为远程访问用户提供专线接入。图 10-48 所示为用路由器做 VPN 服务器时的 Internet 接入区拓扑结构。

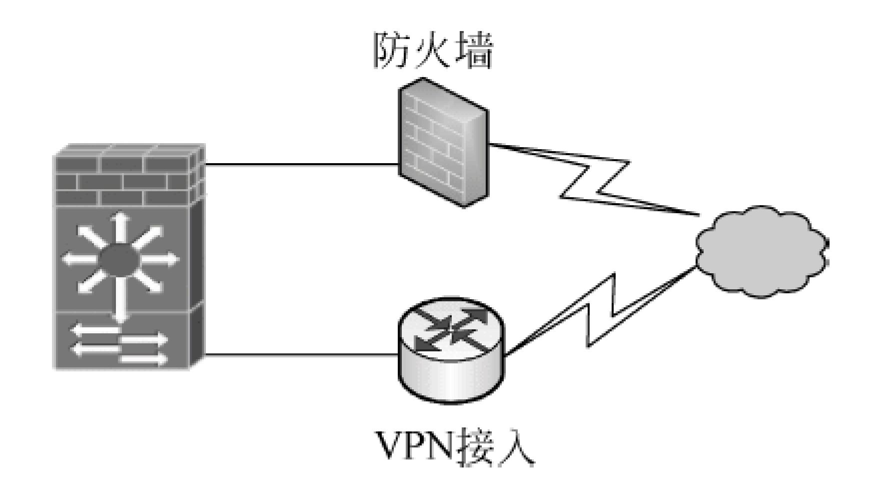


图 10-48 配置路由器 VPN 时的 Internet 接入区示意图

10.4 配置防火墙 VPN

防火墙的主要功能是防御外来入侵,确保内网安全,VPN 只是其附加功能之一。防火墙 VPN 与路由器 VPN 相比,安全性更高。如今大部分防火墙产品都配备了专业管理程序,尤其是不熟悉 CLI 配置方式的用户,只需借助向导即可顺利完成 VPN 的配置。Cisco ASA 5500 系列自适应安全设备是 Cisco 推出的下一代防火墙安全解决方案,它提供了新一代的安全性和 VPN 服务的模块化平台,支持 SSL 加密的远程访问 VPN 和网络互联 VPN。管理员可以通过 Cisco ASDM 以 Web 方式进行远程管理和控制。

10.4.1 配置远程访问 VPN

远程访问 VPN 非常适用于远程移动用户,借助 Internet 或其他公用网络,实现与公司网络的安全、廉价连接。图 10-49 所示为 IPSec VPN 远程访问的拓扑结构。

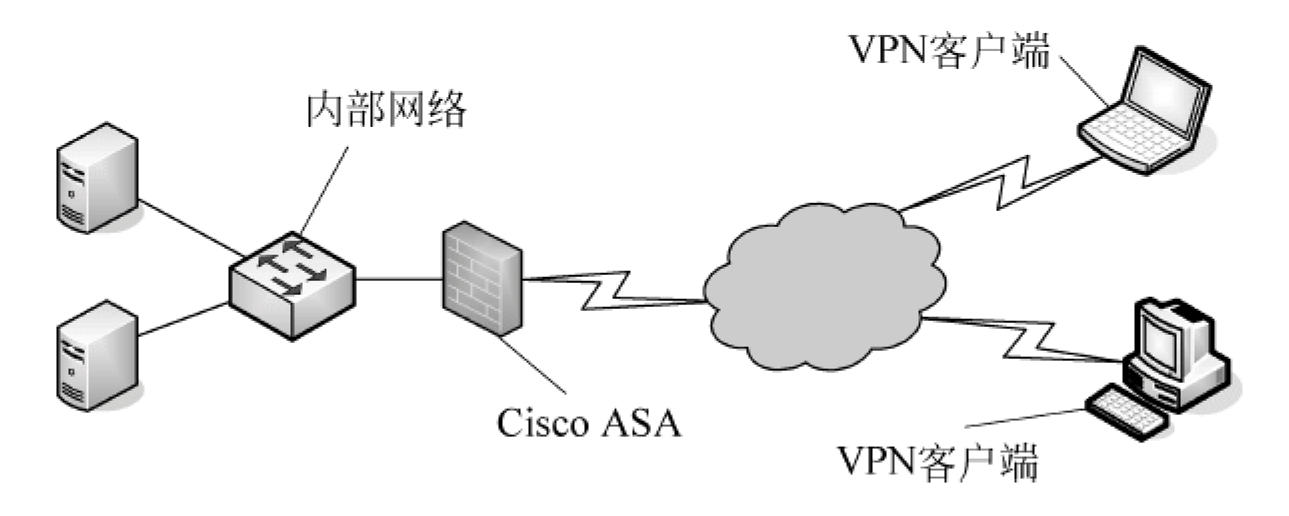


图 10-49 IPSec VPN 远程访问的拓扑结构

在配置 IPSec VPN 远程访问之前,确认已经准备好以下信息。

(1) IPSec VPN 远程客户端使用的 IP 地址池范围。

(2) 在本地认证数据库中创建用户列表,或者使用 AAA 服务器实现认证。

当 VPN 连接时,远程客户端使用的网络信息如下。

(1) 主 DNS 服务器和辅 DNS 服务器的 IP 地址。

(2) 默认域名。

(3) 认证远程客户端可访问的本地主机、组和网络的 IP 地址列表。

在任意远程管理终端上运行 Cisco ASDM,初始化配置过程中,Cisco ASA 5510 的 VPN 就已经被分配了专用的外部接口地址,管理员通过该 IP 地址即可实现远程 Web 连

接。在主窗口中单击 Configuration 按钮，在左侧列表框中选择 Remote Access VPN 选项，配置远程访问 VPN，如图 10-50 所示。VPN 向导有两种：Startup Wizard(启动向导)和 SSL VPN Wizard(SSL VPN 向导)。

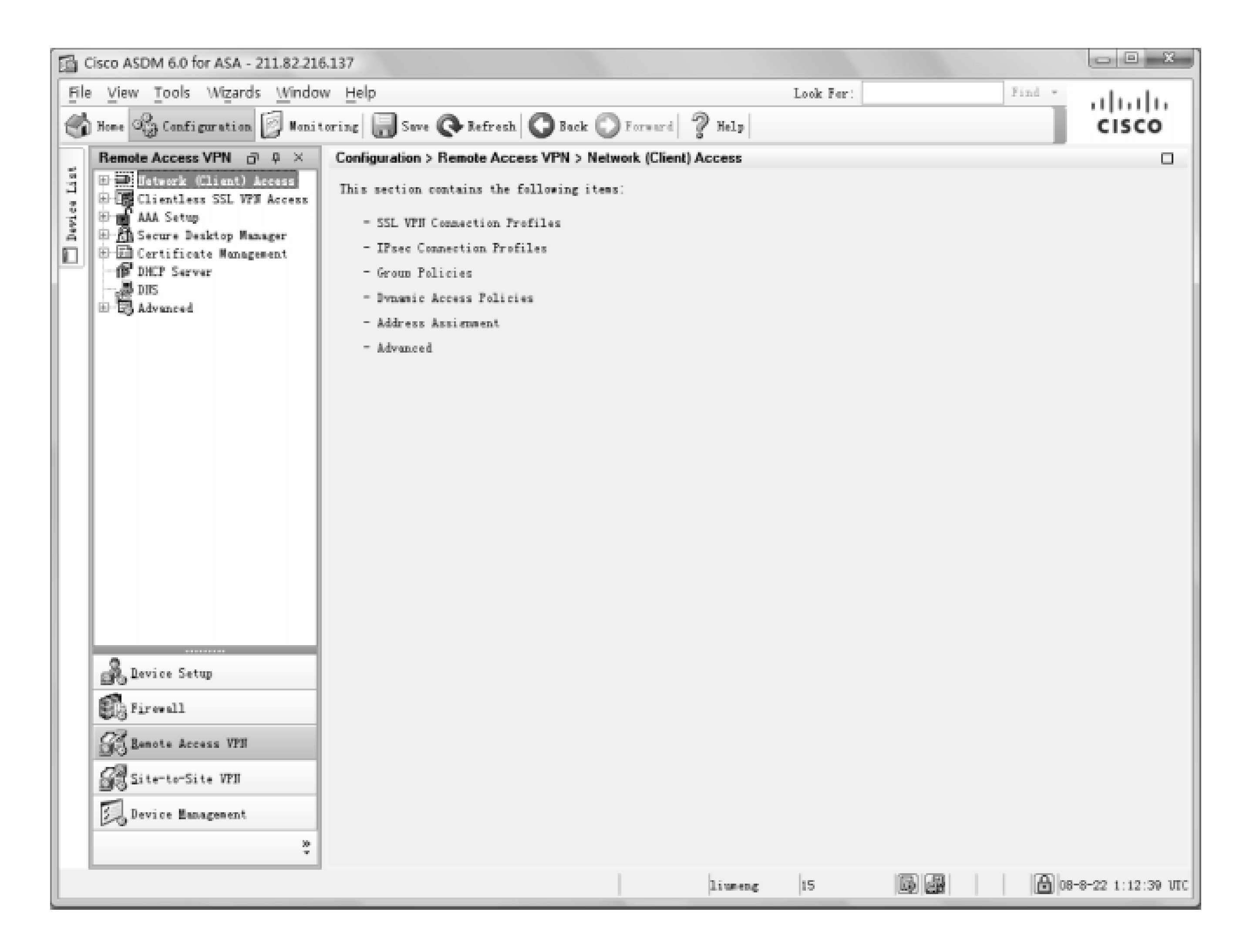


图 10-50　Remote Access VPN 选项

1. 运行 SSL VPN 配置向导

运行 SSL VPN 配置向导的操作步骤如下。

(1) SSL VPN 配置向导的启动方式与启动向导类似，打开 Remote Access VPN 对话框，并在 Wizard 菜单栏中选择 SSL VPN Wizard 命令，显示如图 10-51 所示的 SSL VPN Connection Type 对话框。系统默认选中 Clientless SSL VPN Access 复选框，即只为通过基于浏览器(Windows 内置客户端)访问 VPN 的客户端启用 SSL 加密传输。如果网络中存在使用 Cisco 专用客户端(AnyConnect VPN Client)的用户，建议同时选中 Cisco SSL VPN Client 复选框。

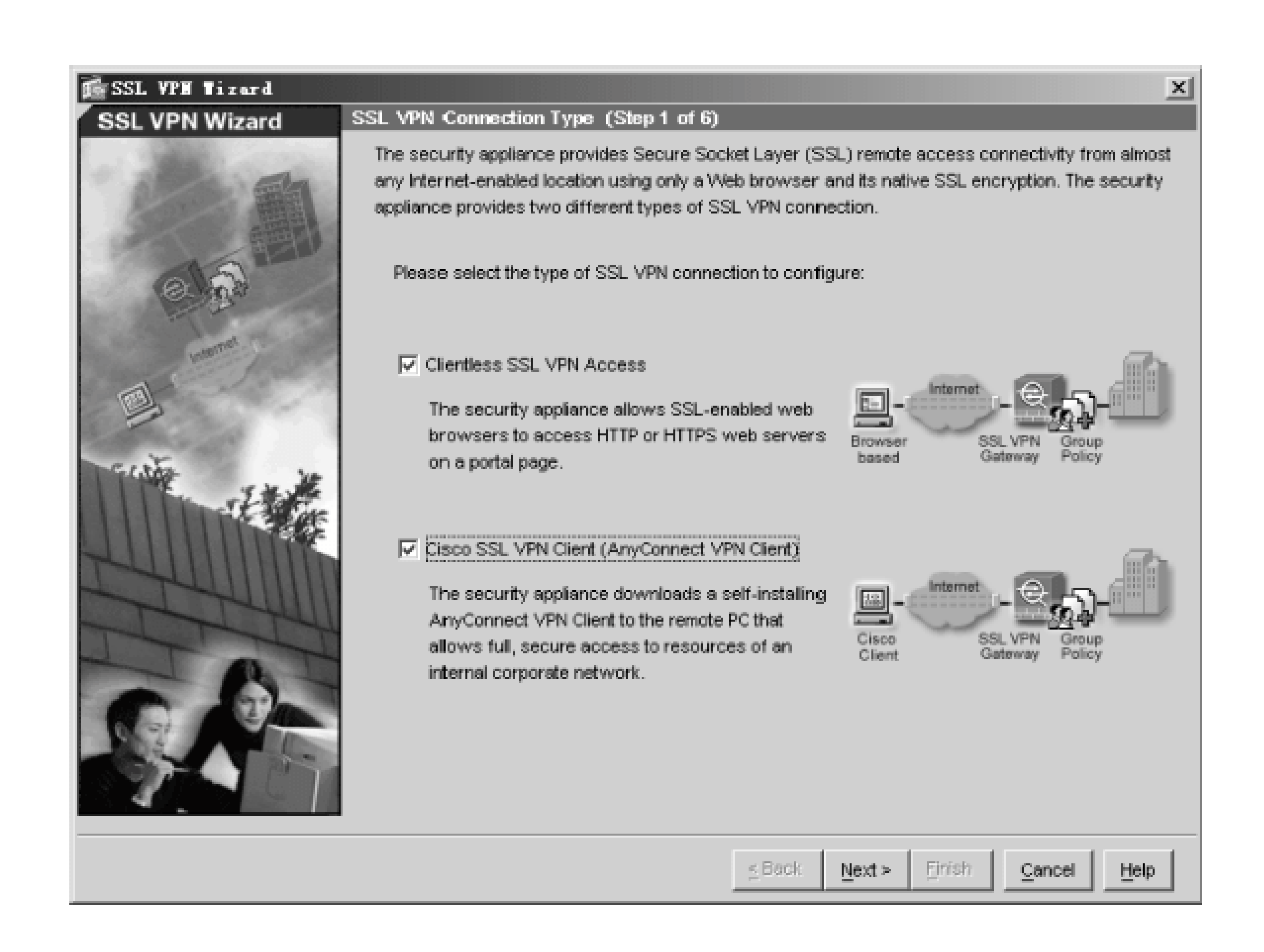


图 10-51　SSL VPN Connection Type 对话框

(2) 单击 Next 按钮，显示如图 10-52 所示的 SSL VPN Interface 对话框，在 Connection Name 文本框中输入 VPN 连接名称，在 SSL VPN Interface 下拉列表框中选择 outside 选项，即用户访问此 VPN 时使用的接口。

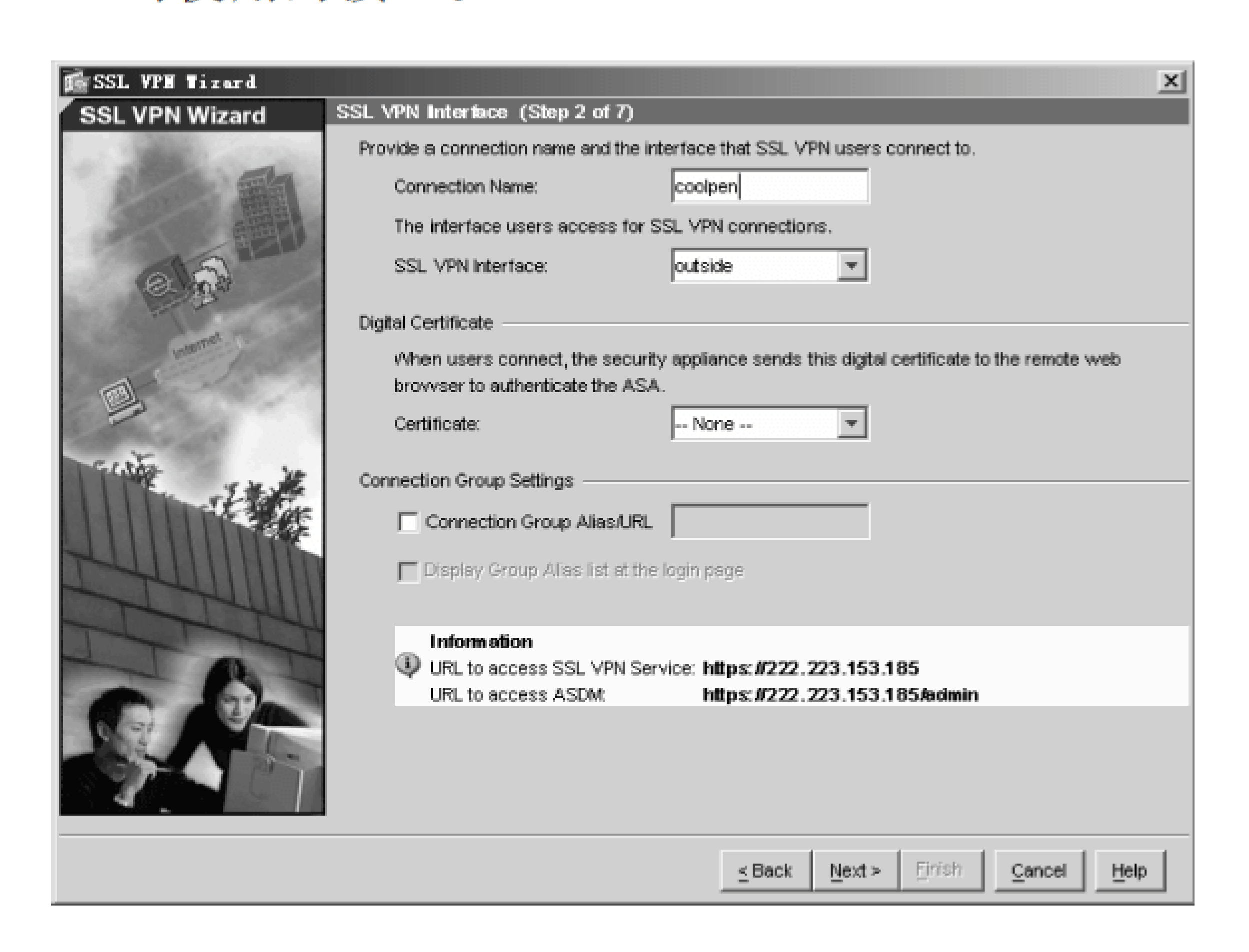


图 10-52　SSL VPN Interface 对话框

(3) 单击 Next 按钮，显示如图 10-53 所示的 User Authentication 对话框，系统默认选中 Authenticate using a AAA server group 单选按钮，即使用 AAA 服务器验证来访用户身份。如果选中 Authenticate using the local user database 单选按钮，即使用本地用户账户数据库验证，则既可以在这里创建新用户账号，也可以稍后使用 ASDM 配置界面添加用户。在 Username、Password 和 Confirm Password 文本框中分别输入用户名、密码和确认密码，单击 Add 按钮，即可向本地用户数据库中添加新的用户。重复操作，可添加多个用户。

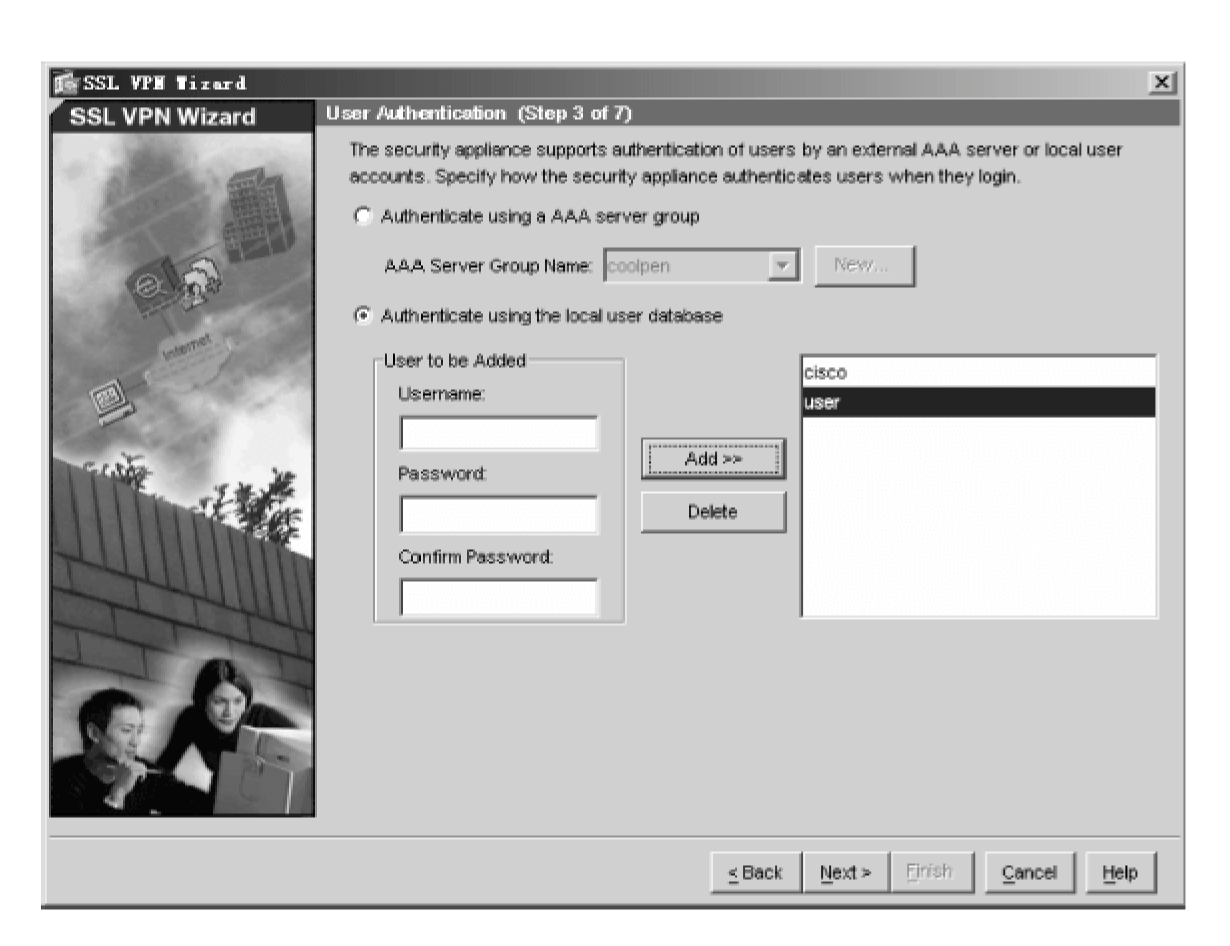


图 10-53　User Authentication 对话框

(4) 单击 Next 按钮，显示如图 10-54 所示的 Group Policy 对话框，选中 Create new group policy 单选按钮，并在其对应文本框中输入名称，即可创建新的组策略。建议不要修改系统默认策略，以免影响到其他访问功能的应用。



图 10-54 Group Policy 对话框

(5) 单击 Next 按钮，显示如图 10-55 所示的 Clientless Connections Only-Bookmark List 对话框，设置 VPN 客户端访问页面中的链接列表，即用户登录 VPN 后可以快速访问的 Web 站点或网络资源。

(6) 单击 Manage 按钮，显示如图 10-56 所示的 Configure GUI Customization Objects 对话框，配置 SSL VPN 门户网站页面显示的可用资源或站点书签列表。



图 10-55 Clientless Connections Only-Bookmark List 对话框

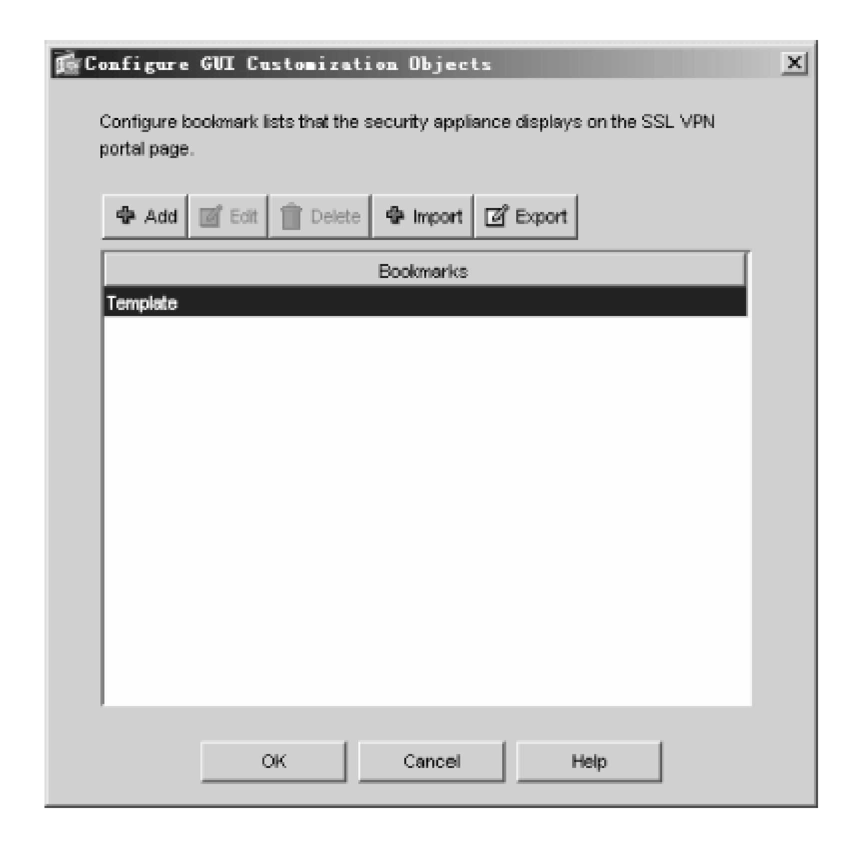


图 10-56 Configure GUI Customization Objects 对话框

(7) 单击 Add 按钮，显示如图 10-57 所示的 Add Bookmark List 对话框，编辑现有书签列表。在 Name 和 URL 栏中分别可以设置显示名称和对应的 URL 路径。

(8) 单击 Add 按钮，显示如图 10-58 所示的 Add Bookmark Entry 对话框，添加书签项。

(9) 连续单击 OK 按钮，返回 Clientless Connections Only-Bookmark List 对话框，所选对象已经显示在下拉列表框中。单击 Next 按钮，显示如图 10-59 所示的 IP Address Pools and Client image-AnyConnect VPN Client Connections Only 对话框，为通过 SSL VPN 拨入的用户创建 IP 地址池，并为其提供 VPN 客户端安装程序。

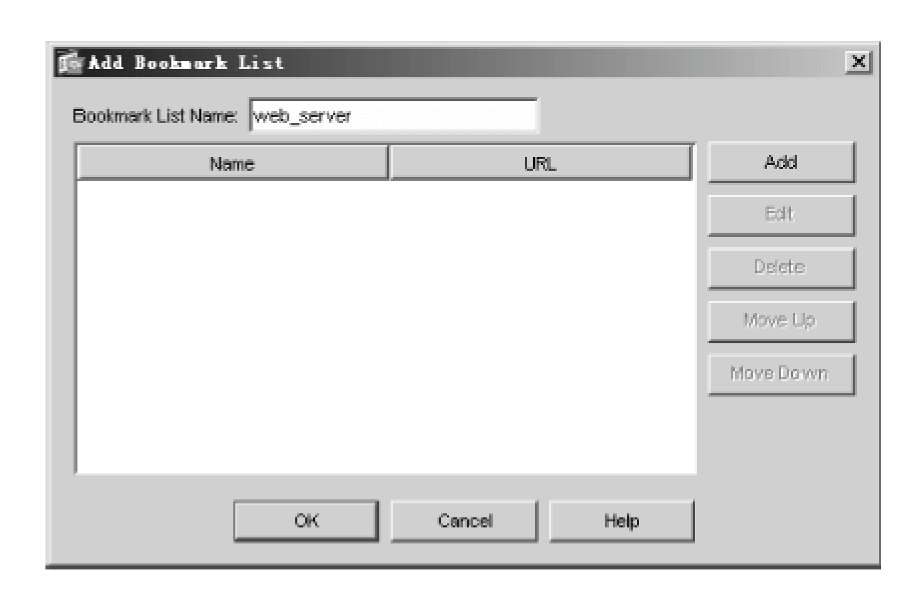


图 10-57 Add Bookmark List 对话框

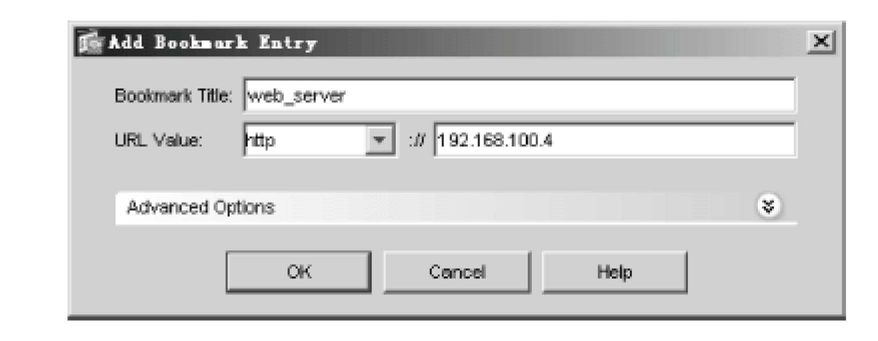


图 10-58 Add Bookmark Entry 对话框

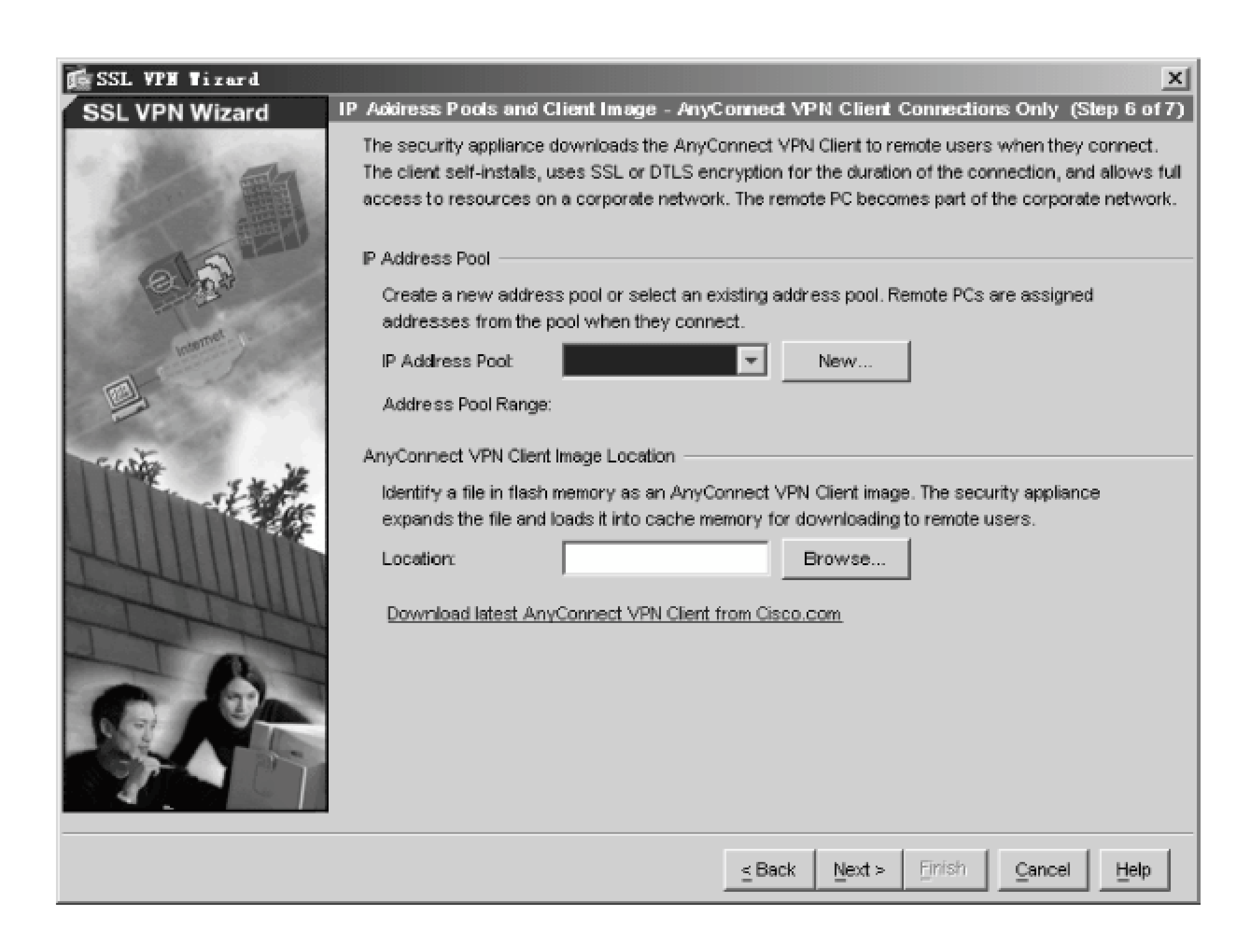


图 10-59 IP Address Pools and Client image-AnyConnect VPN Client Connections Only 对话框

（10）单击 IP Address Pool 下拉列表框后的 New 按钮，显示如图 10-60 所示的 Add IP Pool 对话框，输入地址池名称和起止 IP 地址即可，单击 OK 按钮返回到 SSL VPN 配置向导。

（11）在 IP Address Pools and Client image-AnyConnect VPN Client Connections Only 对话框中，单击 Browse 按钮，显示如图 10-61 所示的 Add SSL VPN Client Image 对话框，选择将要为拨入用户提供的客户端安装程序。如果 ASA 缓存中已经包含 VPN 客户端程序，则可以单击 Browse Flash 按钮查找，否则可以上传本地计算机上的客户端安装程序。



图 10-60 Add IP Pool 对话框

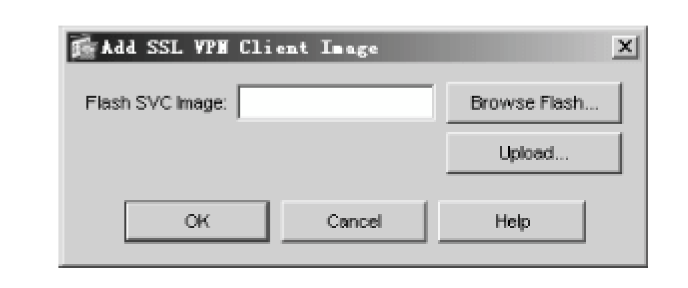


图 10-61 Add SSL VPN Client Image 对话框

（12）单击 Upload 按钮，显示如图 10-62 所示的 Upload Image 对话框，单击 Browse Local Files 按钮，显示 Select 对话框，选择希望上传的客户端安装程序并单击 Select 按钮即可。

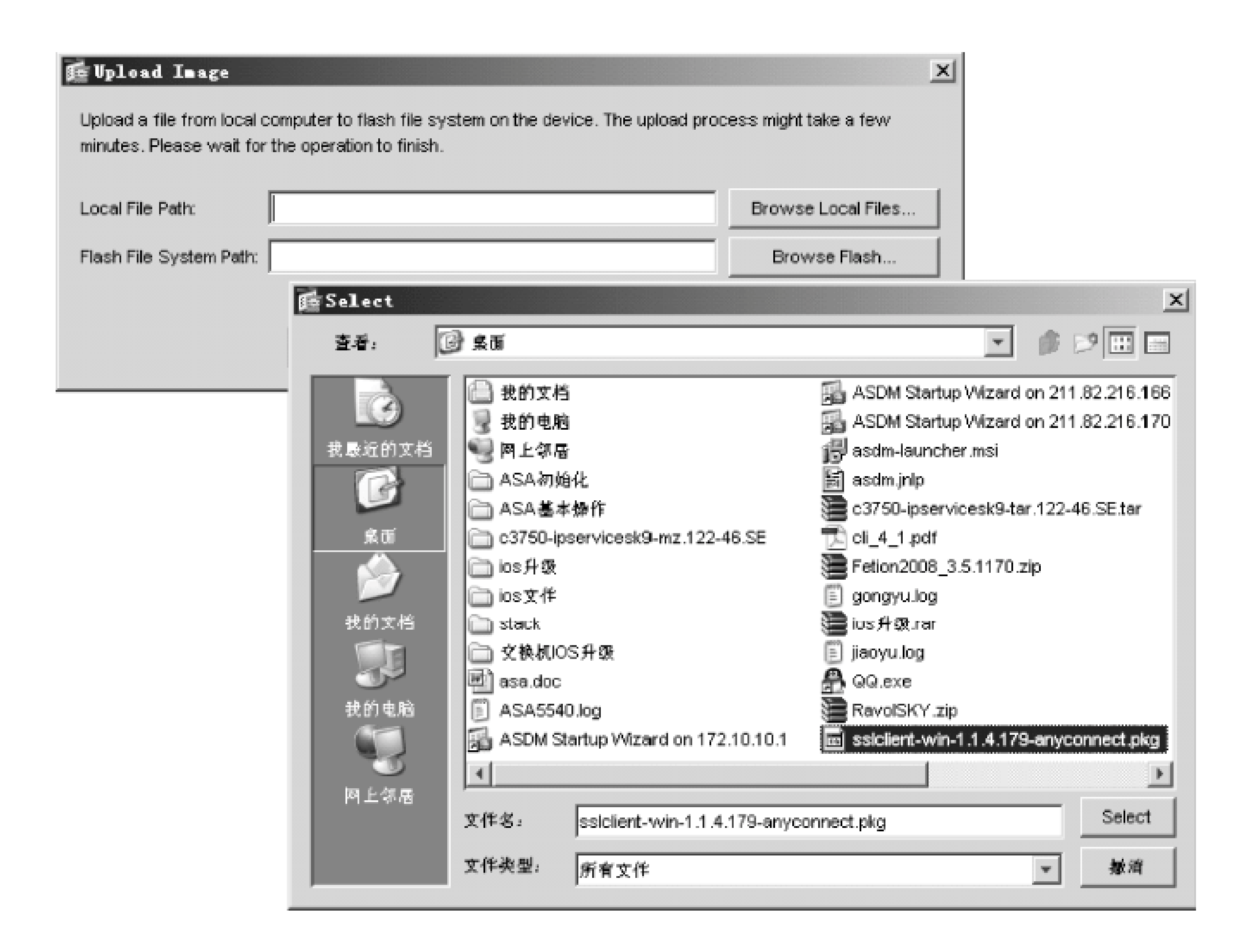


图 10-62　Upload Image 对话框

（13）单击 Next 按钮，显示如图 10-63 所示的 Summary 对话框，显示已创建 SSL VPN 摘要信息。单击 Finish 按钮，完成 SSL VPN 配置并保存。



图 10-63　Summary 对话框

2. 配置 NAT

完成 SSL VPN 配置向导之后，外部用户虽然可以通过 VPN 拨叫到内网，但由于 ASA 地址池为客户端分配的 IP 地址，并不能通过核心交换机路由到其他网络，因此还必须通过 NAT 将其转换为能够访问内部网络资源的 IP 地址。

（1）在 ASDM 管理窗口中单击 Configuration 按钮，在左侧导航栏中单击 Firewall 按钮，选择 Firewall 分支下的 NAT Rules 选项，显示如图 10-64 所示的窗口。

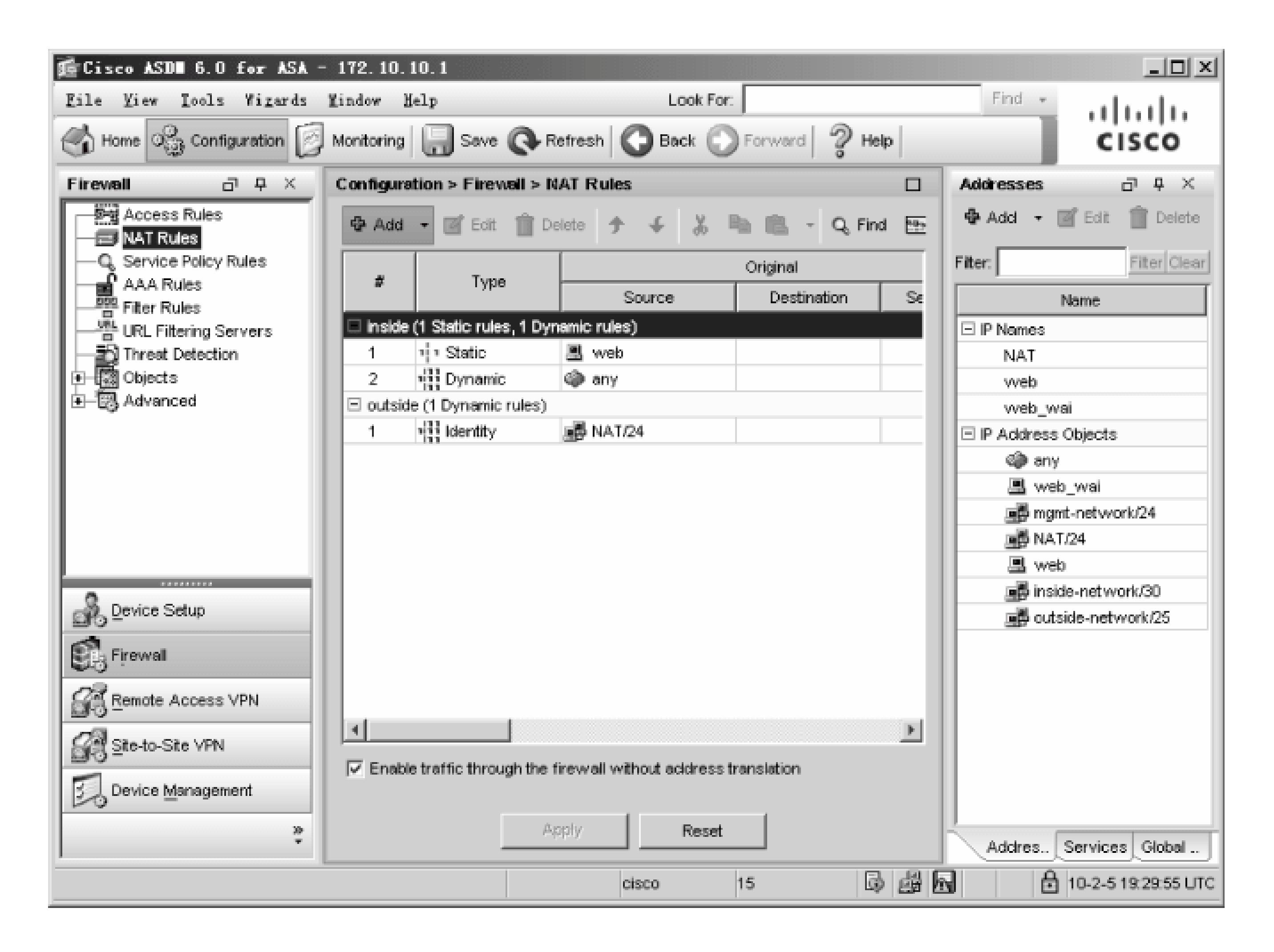


图 10-64　ASDM 管理窗口

（2）单击 Add 按钮并选择下拉菜单中的 Add Dynamic NAT Rule 选项，显示如图 10-65 所示的 Add Dynamic NAT Rule 对话框，在 Interface 下拉列表框中选择 inside 选项。

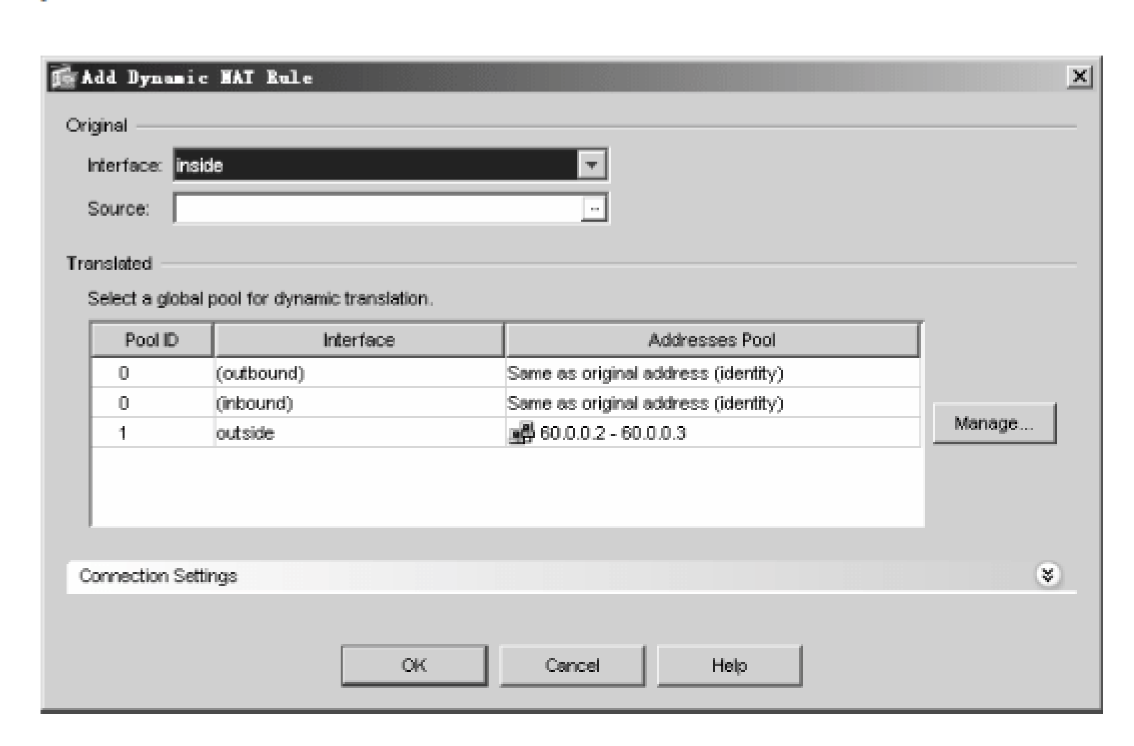


图 10-65　Add Dynamic NAT Rule 对话框

（3）单击 Source 文本框后的"…"按钮，显示如图 10-66 所示的 Browse Source 对话框，如果源地址列表中已经存在希望添加的网络，即为拨入用户创建的地址池，则可以直接选择。否则，需要立即创建。

（4）单击 Add 按钮并选择下拉菜单中的 IP Name 选项，显示如图 10-67 所示的 Add IP Name 对话框，输入源地址名称、IP 地址和描述信息即可。单击 OK 按钮，将其添加到源列表中。

（5）在 Browse Source 对话框中选中刚刚创建的源"SSL VPN_Pool"，单击"确定"按钮返回 Add Dynamic NAT Rule 对话框，单击 OK 按钮保存配置，配置结果如图 10-68 所示。

（6）在 ASDM 管理窗口的右侧边栏底部单击 Global 按钮，在 Global 选项卡中单击 Add 按钮，显示如图 10-69 所示的 Add Global Address Pool 对话框，在 Interface 下拉列表框中选择 outside 选项，默认情况下此时 Pool ID 文本框中将自动输入 1，如果在此之前已经

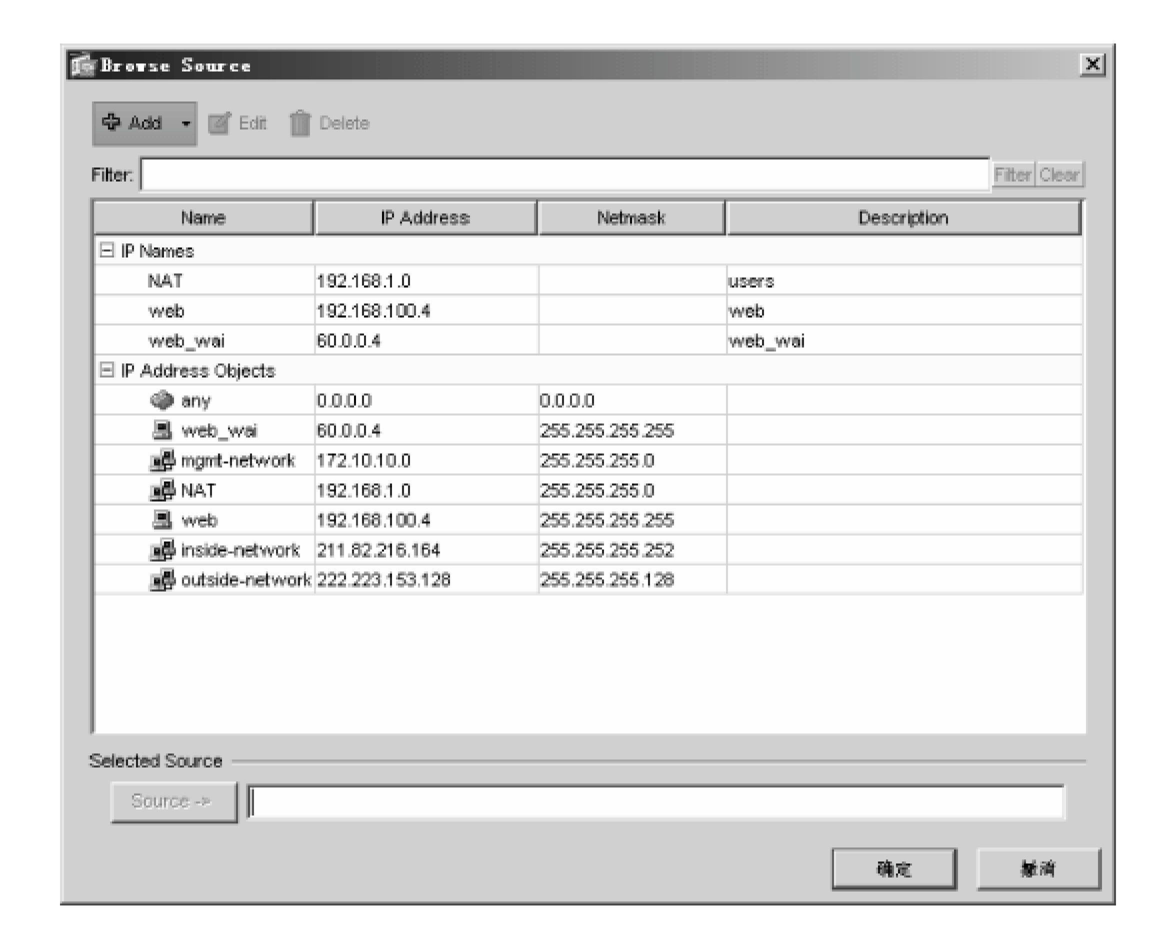


图 10-66　Browse Source 对话框

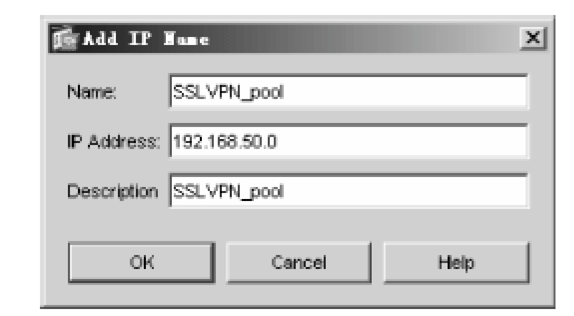


图 10-67　Add IP Name 对话框

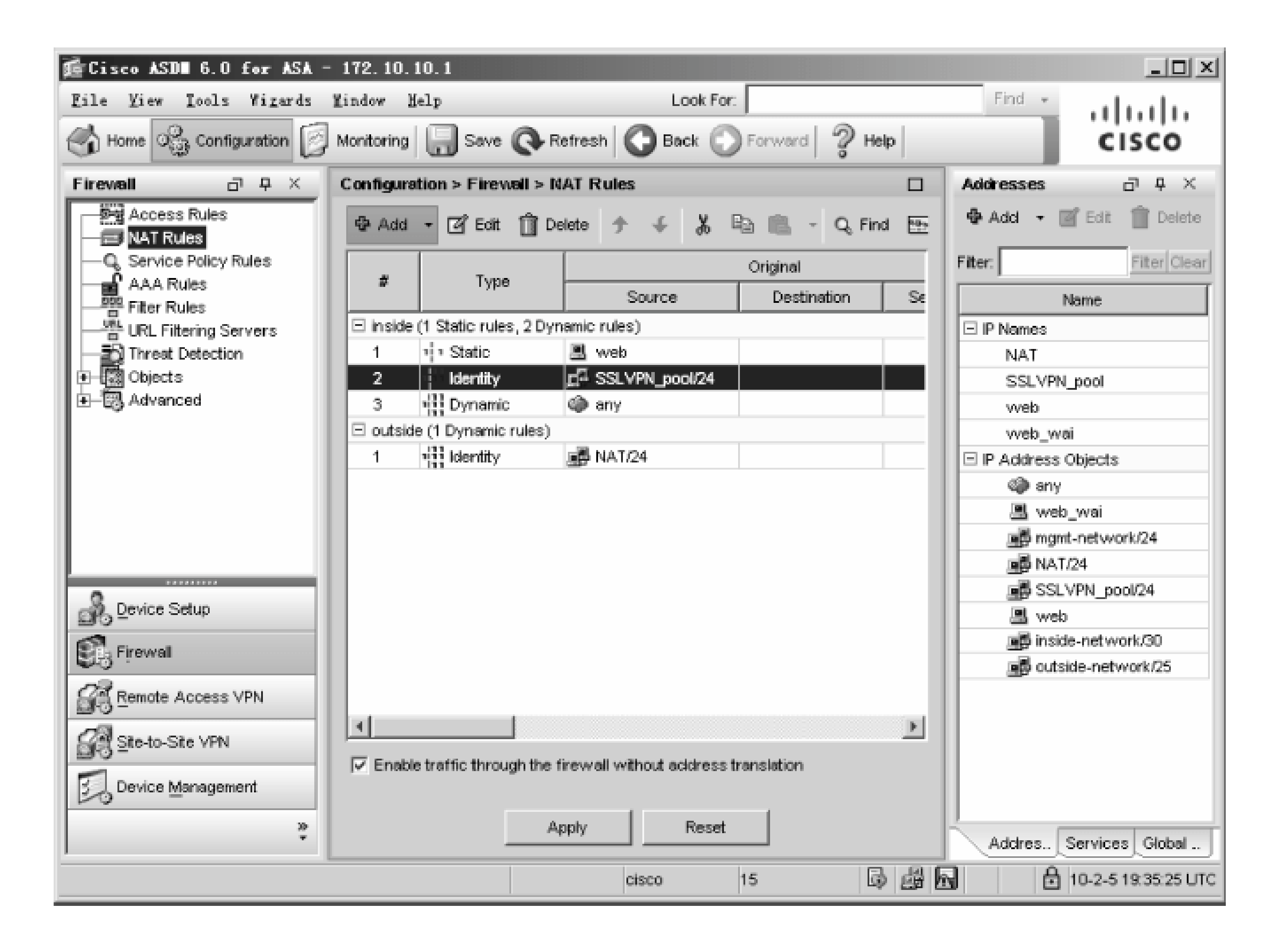


图 10-68　成功创建的动态 NAT 规则

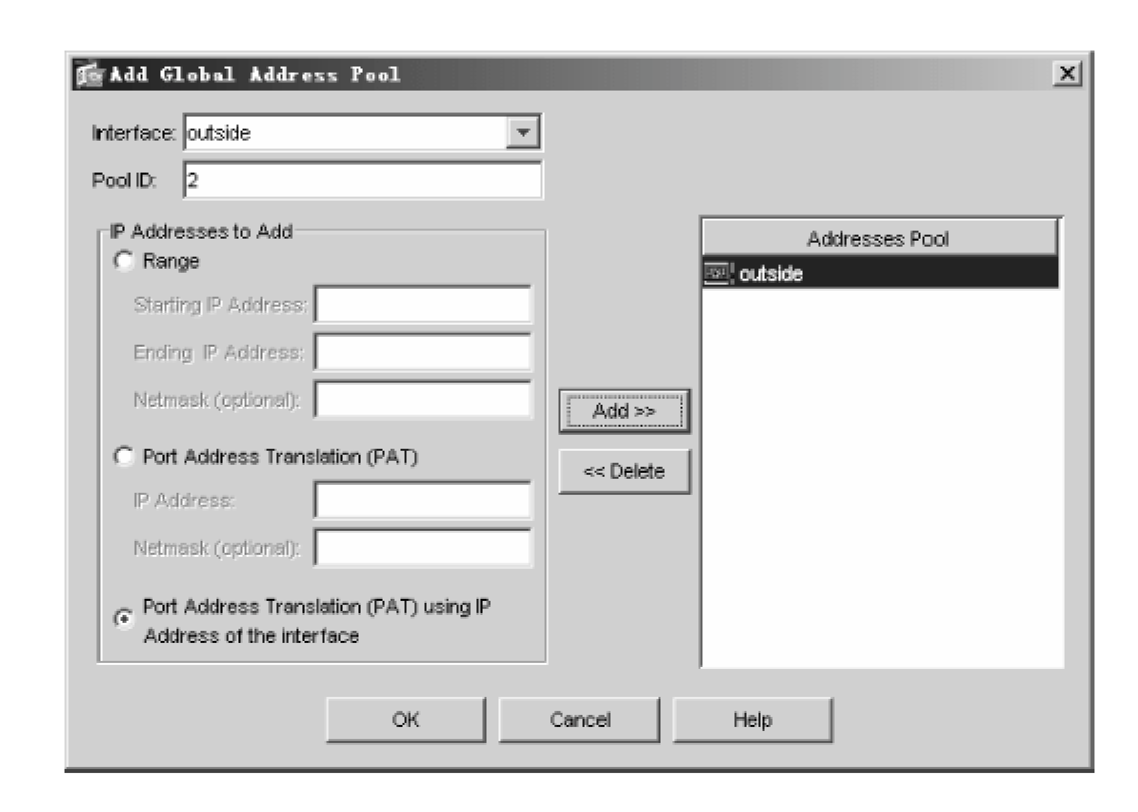


图 10-69　Add Global Address Pool 对话框

创建过全局地址池,则此处将以此类推。然后选中 Port Address Translation(PAT) using IP Address of the interface 单选按钮即可。

(7) 单击 OK 按钮,保存配置并返回 ASDM 管理窗口,配置结果如图 10-70 所示。

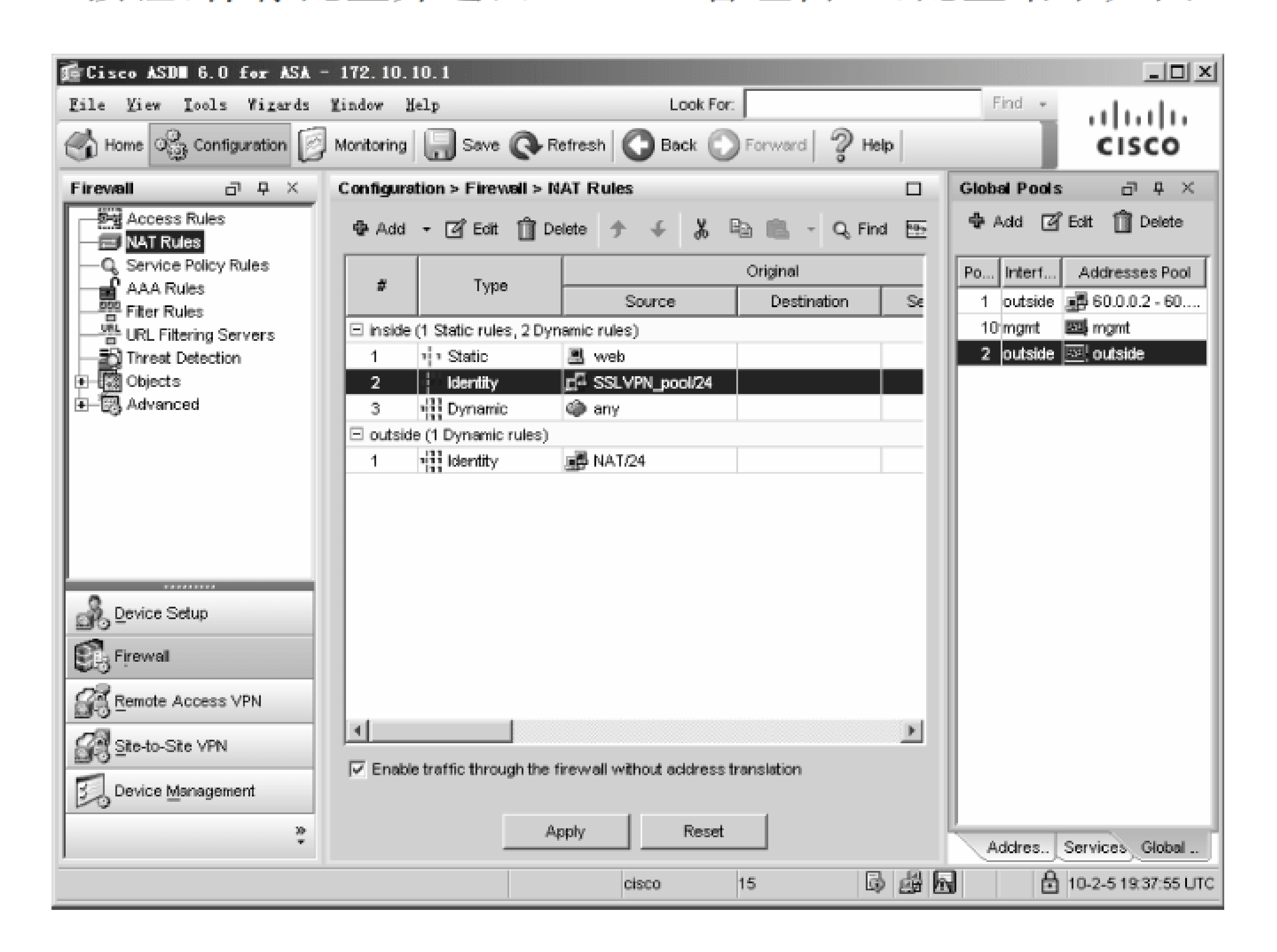


图 10-70 成功创建的全局地址池

3. 配置非转换 NAT

创建非转换 NAT 规则的过程与创建动态 NAT 规则基本类似,具体操作步骤如下。

(1) 单击 Add 按钮并选择下拉菜单中的 Edit NAT Exempt Rule 选项,显示如图 10-71 所示的 Edit NAT Exempt Rule 对话框,选中 Exempt 单选按钮,在 Interface 下拉列表框中选择 inside 选项。

(2) 单击 Source 文本框后的"…"按钮,显示如图 10-72 所示的 Browse Source 对话框,在 IP Address Objects 选项区域内选择 any 选项。

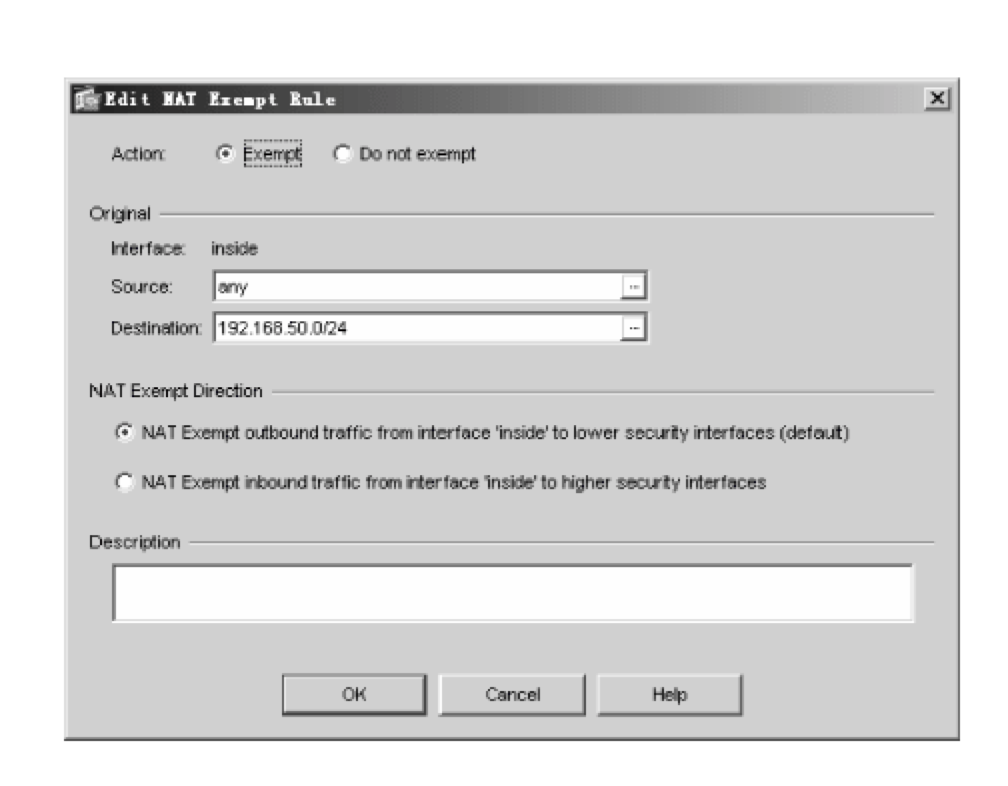


图 10-71 Edit NAT Exempt Rule 对话框

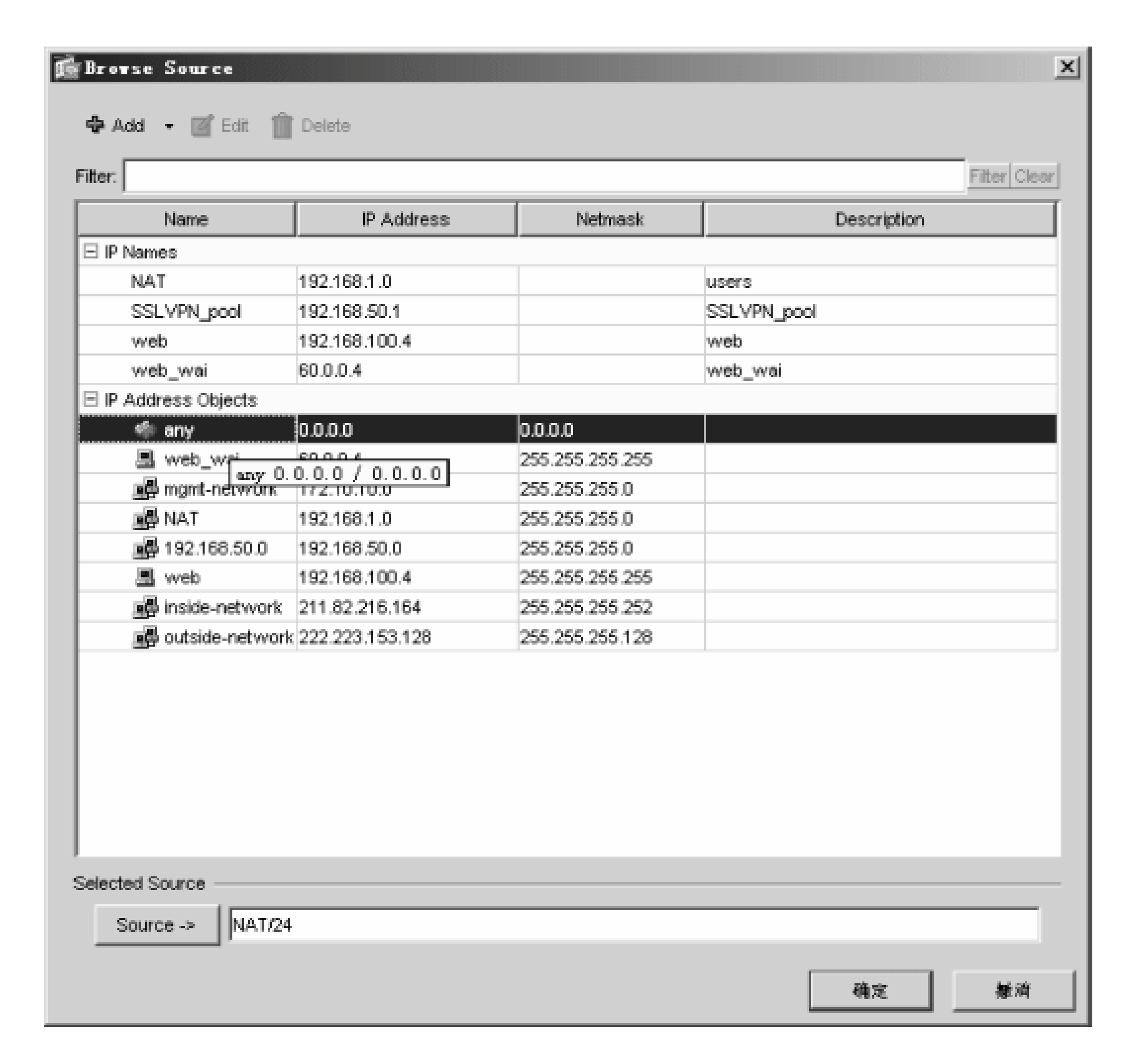


图 10-72 Browse Source 对话框

(3) 依次单击“确定”和 OK 按钮，保存配置并返回到 ASDM 管理窗口，配置结果如图 10-73 所示。

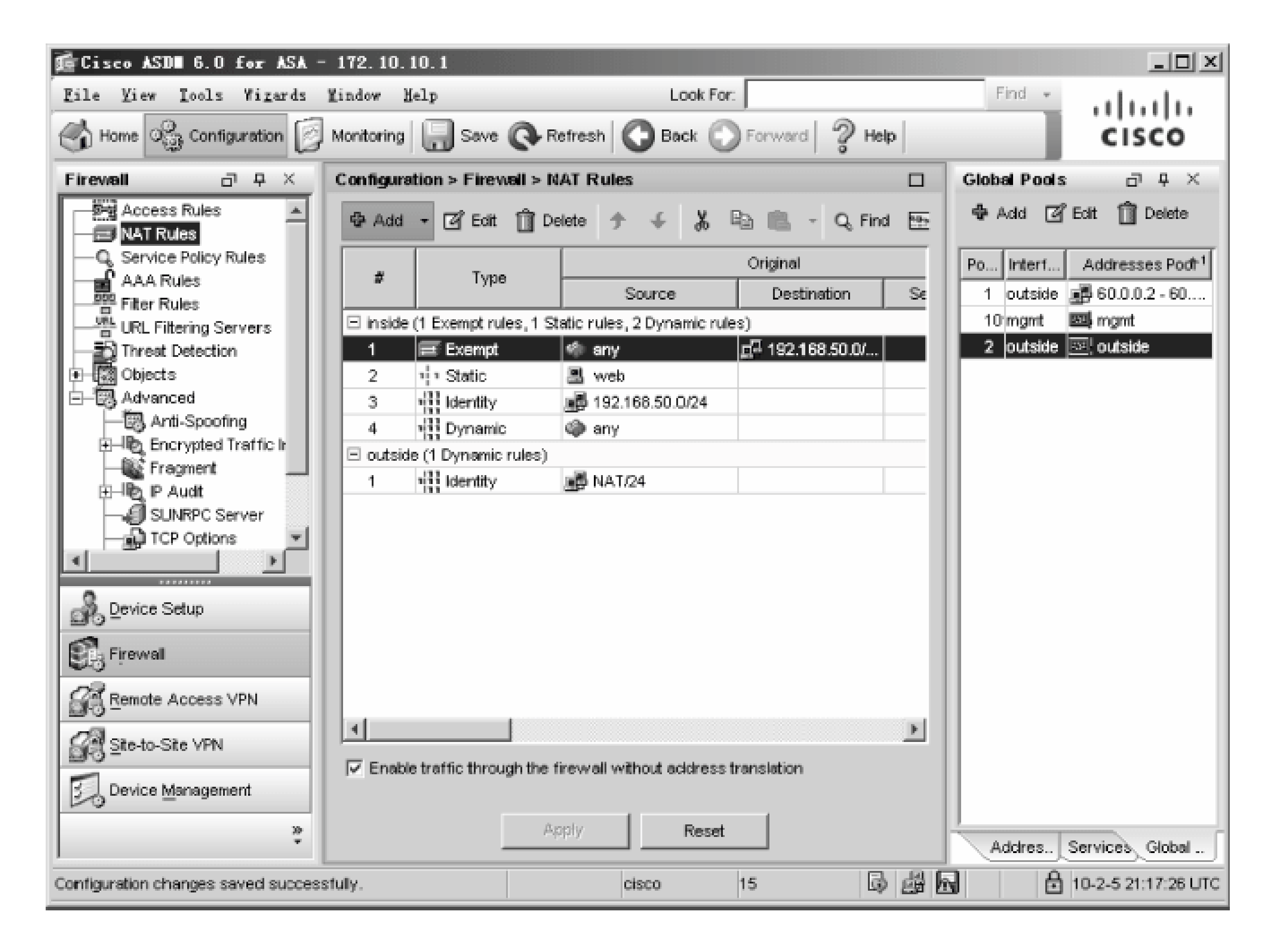


图 10-73 成功创建的非转换 NAT 规则

10.4.2 Cisco AnyConnect VPN 客户端

Cisco AnyConnect VPN 客户端相对于 Windows 系统集成的 VPN 客户端而言更加简便，用户使用 IE 浏览器访问 VPN 时，即可提示用户下载，下载过程中将自动安装。当然用户也可以通过 Internet 下载该客户端安装程序。

(1) 在 IE 浏览器地址栏中输入 VPN 服务器的地址，如 https://211.82.216.137，正确输入用户名和密码后即可登录，显示如图 10-74 所示的窗口。在客户端下载页面中单击 Start AnyConnect 链接即可开始下载，并自动安装，在此过程中用户需注意浏览器上方的信息栏，安装向导会提示安装 Active 控件。

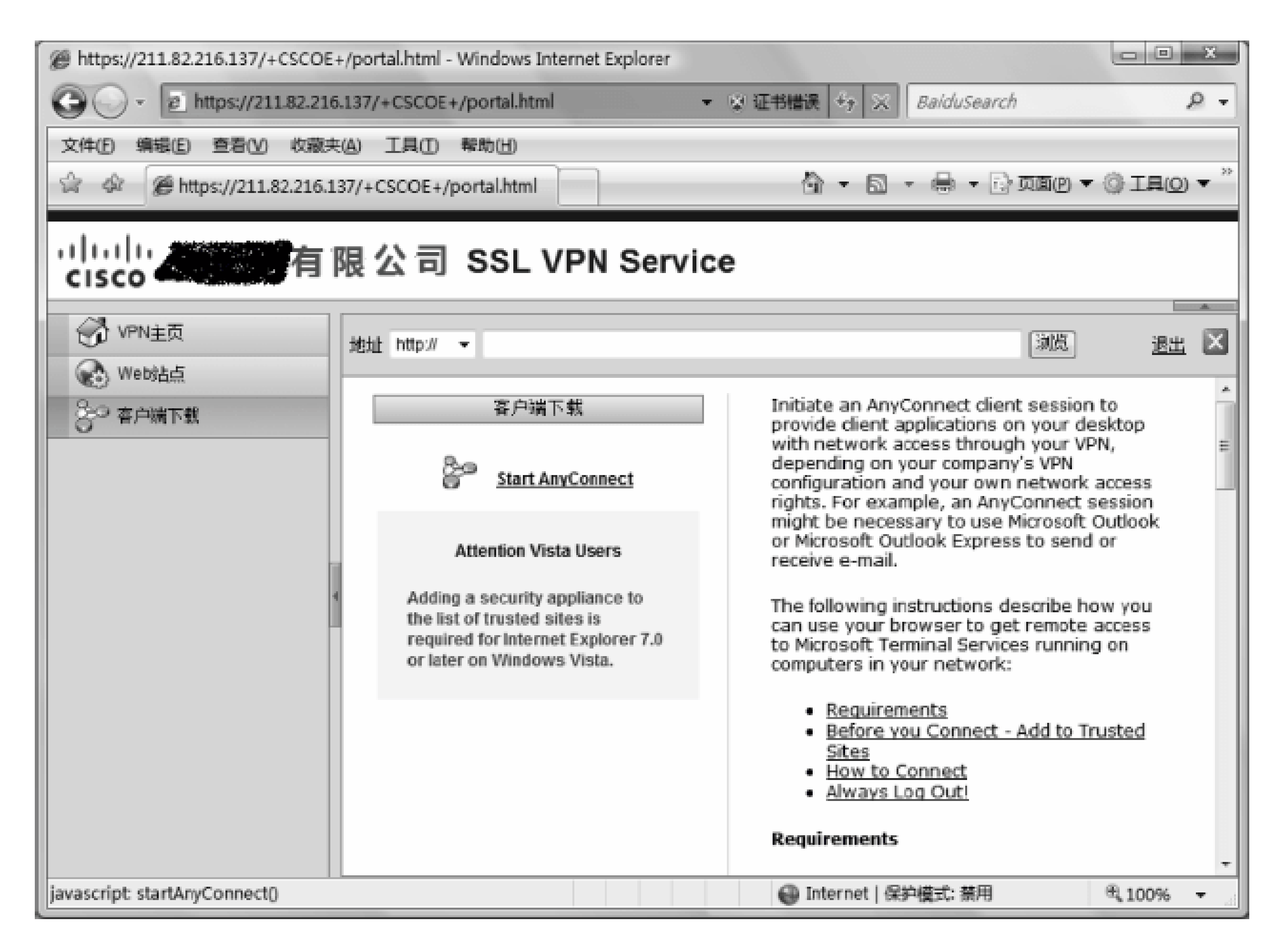


图 10-74 下载并安装 AnyConnect VPN 客户端

(2) 安装完成后将自动连接到远程 VPN 服务器,并在系统任务栏中显示相应提示信息,如图 10-75 所示。

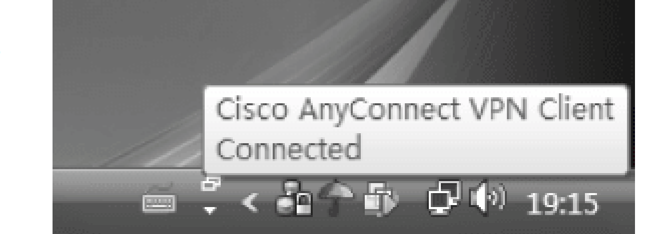


图 10-75 连接到 VPN 服务器

(3) 双击任务栏中的图标,打开 Cisco AnyConnect VPN Client 对话框,默认显示如图 10-76 所示的 Statistics 选项卡,在这里可以查看获得的 IP 地址、VPN 服务器信息、连接时间等。

(4) 右击任务栏中的图标并选择 Quit 或 Disconnect 即可断开 VPN 连接。依次选择"开始"→"所有程序"→Cisco→Cisco AnyConnect VPN Client→Cisco AnyConnect VPN Client 选项,即可启动 AnyConnect VPN 客户端,如图 10-77 所示。



图 10-76 Statistics 选项卡



图 10-77 Connection 选项卡

(5) 在 Connect to 文本框中输入 VPN 服务器的 IP 地址,在 Username 和 Password 文本框中,分别输入用户名和密码,单击 Connect 按钮即可开始连接 VPN 服务器。

10.4.3 知识链接:Cisco ASDM

Cisco ASDM(Adaptive Security Device Manager,自适应安全设备管理器)通过一个直观、易用、基于 Web 的管理界面,提供安全管理和监控服务。结合 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备,Cisco ASDM 提供的智能向导、强大的管理工具和灵活的监控服务,进一步增强 Cisco 安全设备套件提供的先进的集成安全和网络功能,从而加速安全设备的部署。Cisco ASDM 基于 Web 的安全设计,可以使用户能随时随地访问 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备。

10.5 借助 Forefront TMG 实现 VPN

如果要使 Internet 上的用户能够安全地访问公司的内部网络,就可以利用 VPN 服务器来实现。通常,VPN 服务器不能与其他服务"共存"于同一台服务器上,因为在启用 VPN 服务之后,系统默认的路由表发生了改变,不能使用其他的网络通信。不过,部署了 Forefront TMG 以后,既可以将 VPN 服务器安装在 Forefront TMG 服务器上,也可以将内部的 VPN

服务器发布到外部网络。

10.5.1　注意事项

1. 拓扑结构

Forefront TMG 服务器的功能非常强大，VPN 只是其主要应用之一。使用 Forefront TMG 服务器实现远程访问 VPN 时，需要将其部署在网络边缘，直接接入 Internet。虽然 Forefront TMG 服务器本身提供代理服务器和防火墙功能，但考虑到当前企业网络规模较大，并且 Forefront TMG 服务器的性能有限，所以仍保留防火墙作为局域网的 Internet 接入设备。图 10-78 所示为 Forefront TMG 服务器作 VPN 接入时的拓扑结构。

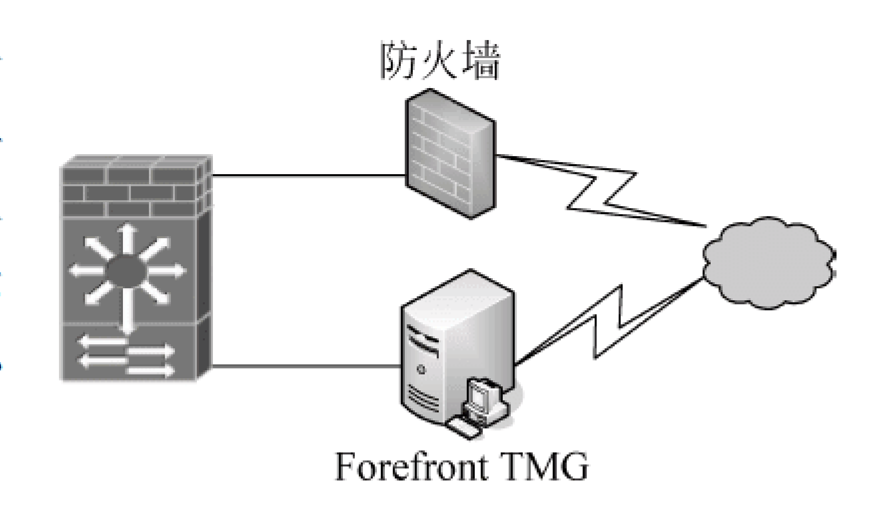


图 10-78　Forefront TMG 服务器作 VPN 接入

2. VPN 服务的发布过程

如果 VPN 服务器安装在 TMG 服务器上，并且要利用网络策略服务器对客户端计算机进行验证，则需按以下步骤进行操作。

(1) 打开“路由和远程访问”控制台，停止“路由和远程访问”服务。

(2) 在 TMG 中配置 VPN 客户端访问，选择要使用的 VPN 协议，并配置 RADIUS 验证。

(3) 创建 VPN 策略，允许来自外网的 VPN 客户端访问 VPN 服务器。

如果 VPN 服务器没有安装在 TMG 服务器上，则只需创建 VPN 发布策略，选择 VPN 服务器协议即可。

10.5.2　配置 VPN 客户端访问

禁用了“路由和远程访问”服务以后，需要在 TMG 中配置 VPN 客户端访问，选择 VPN 协议，并配置 IP 地址分配方式、配置 RADIUS 验证。

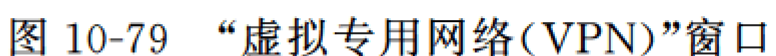
(1) 打开 Forefront TMG 控制台，在左侧栏中选择“虚拟专用网络(VPN)”选项，如图 10-79 所示，在此处即可配置 VPN 服务。

(2) 在右侧的“VPN 客户端任务”选项区域中，单击“配置 VPN 客户端访问”链接，显示如图 10-80 所示的“VPN 客户端 属性”对话框。不过，现在先不要选中“启用 VPN 客户端访问”复选框。

(3) 选择“协议”选项卡，选择远程连接要使用的隧道协议，默认为 PPTP，如图 10-81 所示。如果 VPN 服务器使用 L2TP，则选中“启用 L2TP/IPsec”复选框。

(4) 单击“确定”按钮，返回 TMG 控制台。在“虚拟专用网络(VPN)”窗口右侧的“常规 VPN 配置”选项区域中单击“选择访问网络”链接，显示“虚拟专用网络(VPN)属性”对话框。在“访问网络”选项卡中，选择客户端初始化时连接到的 VPN 服务器的网络，如图 10-82 所示。如果只作为 VPN 服务器对外提供 VPN 接入服务，默认为“外部”；对于站点到站点的连接，则选择“内部”。




图 10-79 “虚拟专用网络(VPN)”窗口

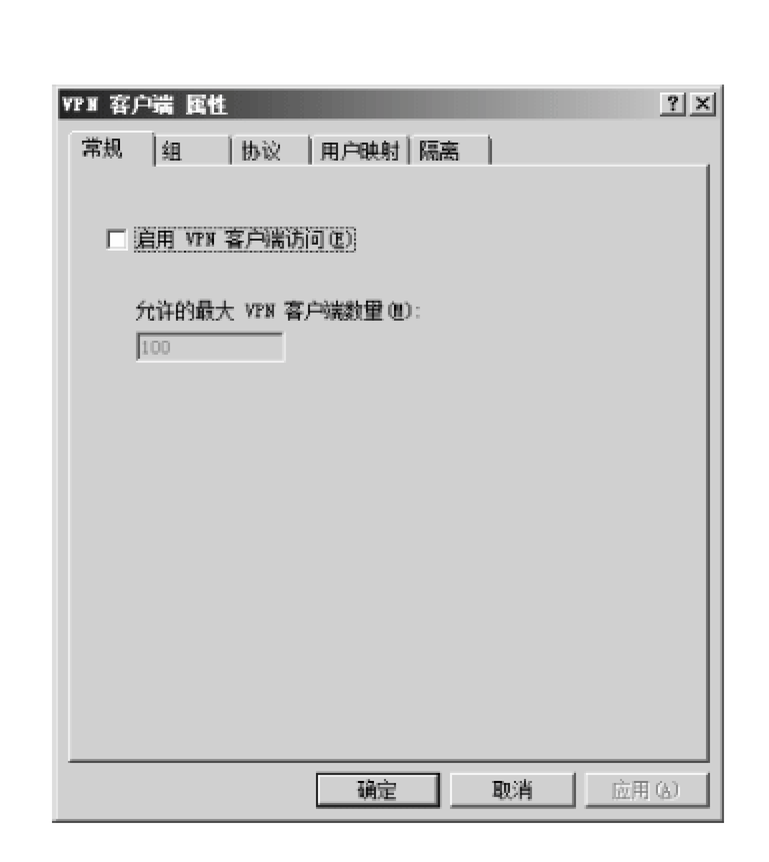


图 10-80 “VPN 客户端 属性”对话框

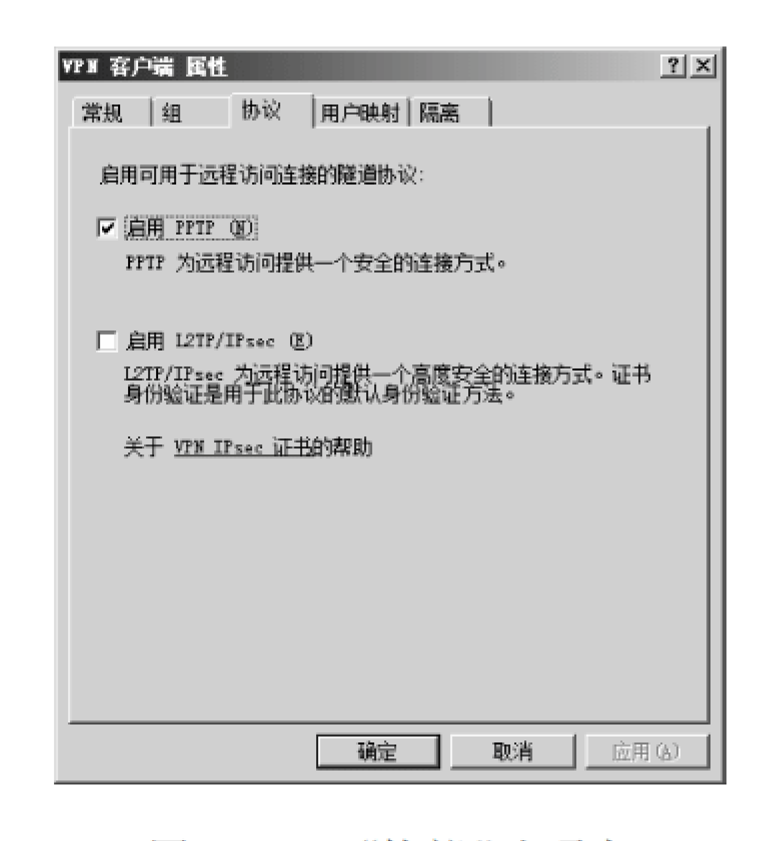


图 10-81 “协议”选项卡

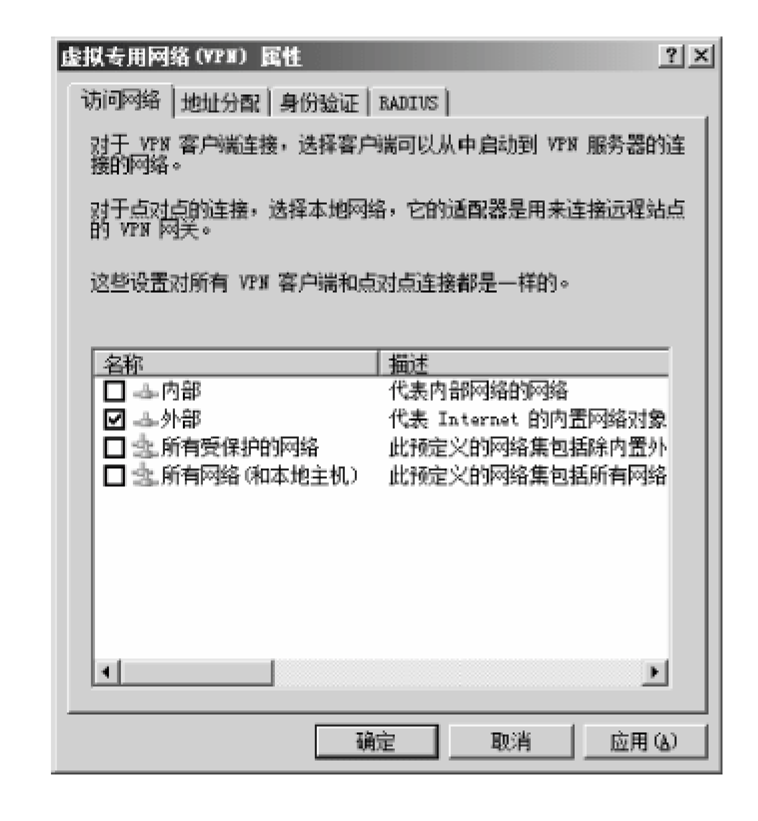


图 10-82 “访问网络”选项卡

(5) 选择“地址分配”选项卡，设置为 VPN 客户端分配 IP 地址的方式。如果要为客户端分配静态 IP 地址，选中“静态地址池”单选按钮，单击“添加”按钮添加 IP 地址段(如图 10-83 所示)；如果网络中存在 DHCP 服务器，则可选中“动态主机配置协议(DHCP)”单选按钮，为客户端分配动态 IP 地址。

注意： 如果配置静态地址，则必须定义一个与本地主机内部网卡不相关的地址段，即地址范围不能与本地主机、外网的子网重复，也不能与路由表中已有的地址冲突。

(6) 如果 VPN 服务器需要使用网络策略服务器对客户端计算机进行验证，则需配置 RADIUS。选择 RADIUS 选项卡，选中“使用 RADIUS 进行身份验证”复选框，如图 10-84 所示。

(7) 单击“RADIUS 服务器”按钮，显示“RADIUS 服务器”对话框，用来添加可用的 RADIUS 服务器。单击“添加”按钮，显示如图 10-85 所示的“添加 RADIUS 服务器”对话框。在“服务器名”文本框中，输入网络策略服务器的 IP 地址。

如果要与网络策略服务器安全地传输数据，还需要设置共享密钥。单击“更改”按钮，显示如图 10-86 所示的“共享的机密”对话框，需要设置密钥。

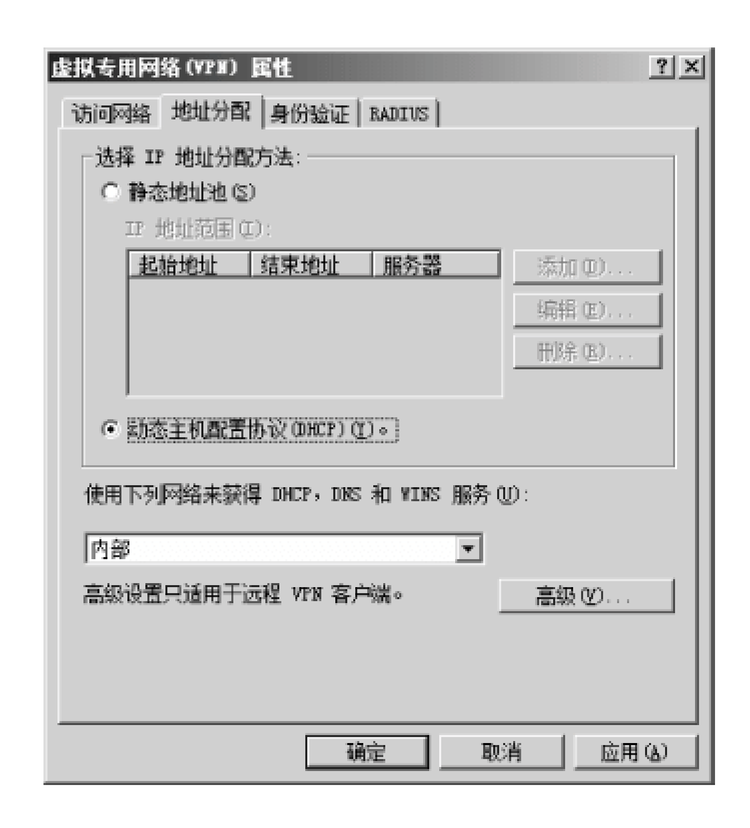


图 10-83 “地址分配”选项卡

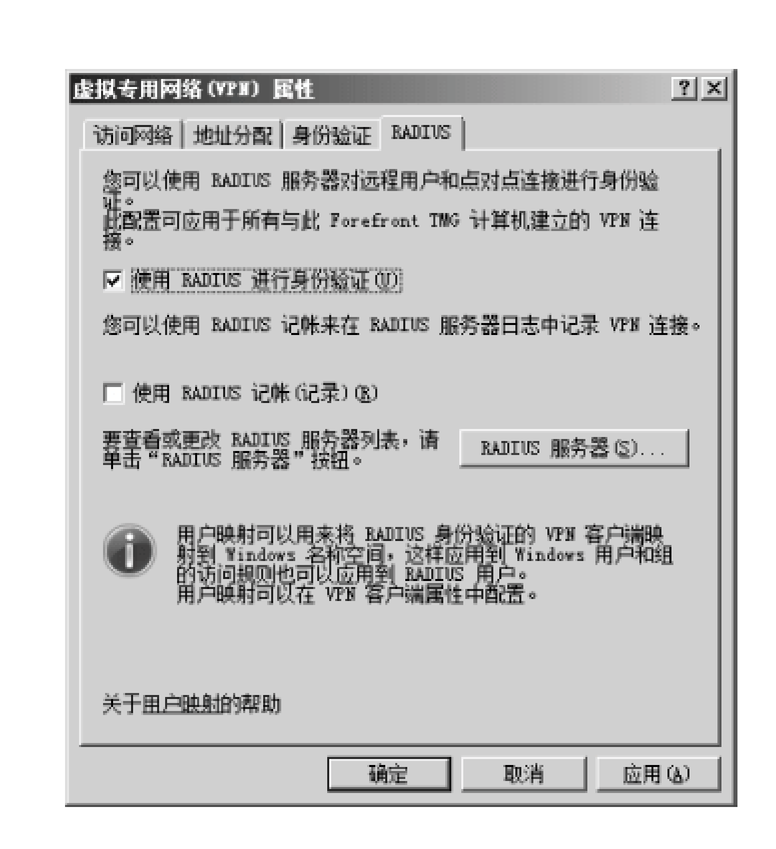
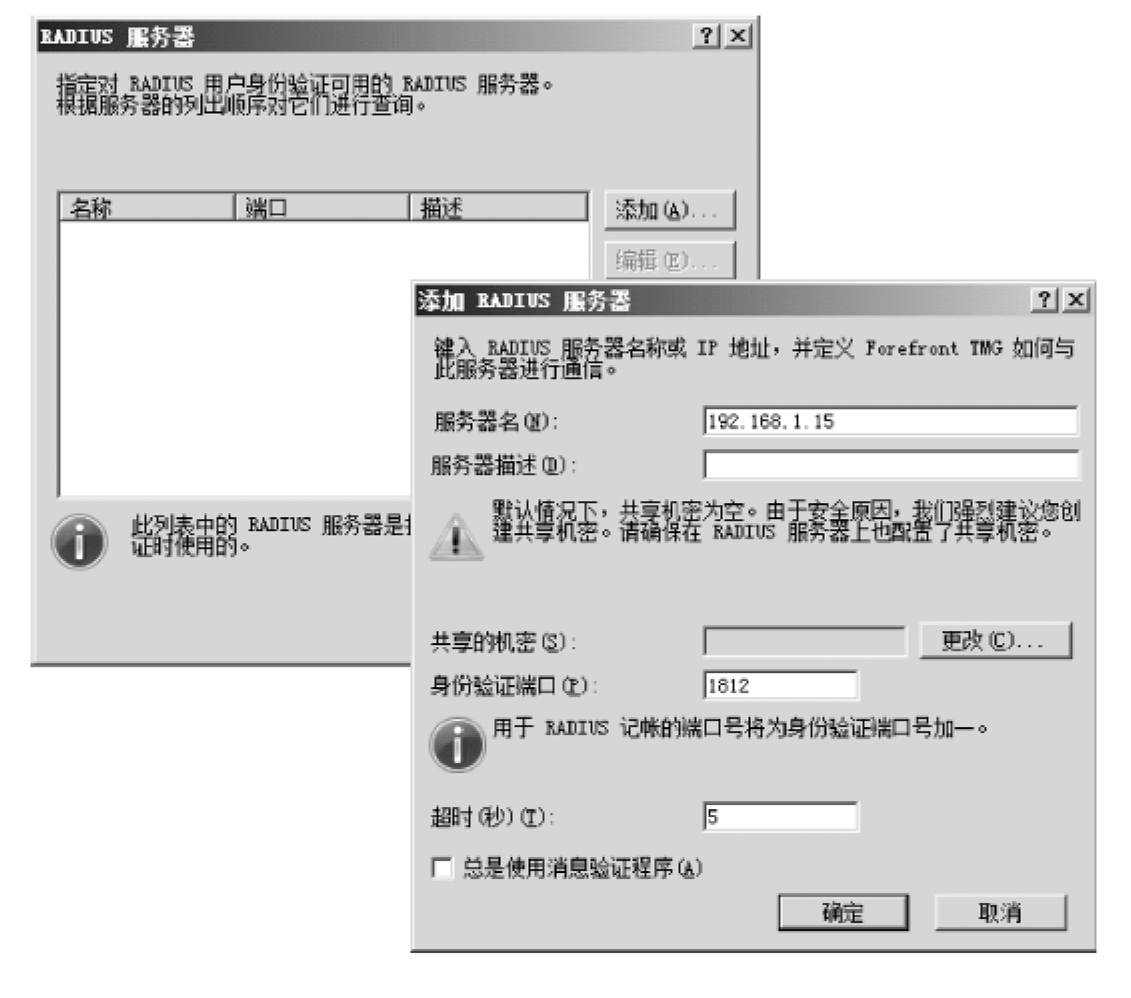


图 10-84 RADIUS 选项卡



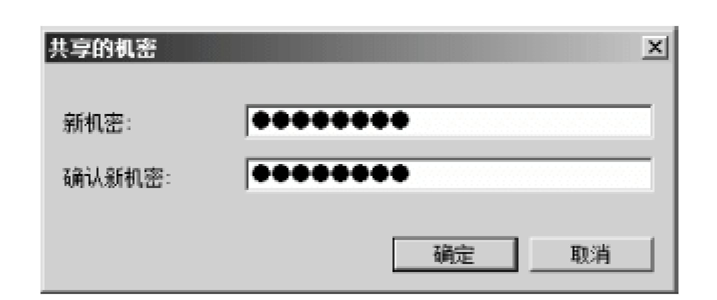


图 10-85 “添加 RADIUS 服务器”对话框

图 10-86 “共享的机密”对话框

(8) 依次单击“确定”按钮保存，并返回 TMG 控制台。然后，在“虚拟专用网络(VPN)”窗口右侧的“VPN 客户端任务”选项区域中单击“启用 VPN 客户端访问”链接。

10.5.3 创建 VPN 服务器发布策略

如果 VPN 服务器位于局域网中，为了使 VPN 客户端能够通过 TMG 防火墙访问 VPN 服务器，还需要在 TMG 中创建一条策略，将 VPN 服务器发布到外网。

(1) 在“防火墙策略”窗口中，启动“新建访问规则向导”。单击“下一步”按钮，在“规则操作”对话框中选中“允许”单选按钮。

(2) 单击“下一步”按钮，显示“协议”对话框。如果 VPN 服务器安装在当前 TMG 服务器上，在“此规则应用到”下拉列表框中选择“所有出站通讯”选项即可；如果 VPN 服务器在内部网络中，则需在“此规则应用到”下拉列表框中选择“所选的协议”选项，并单击“添加”按钮，添加所使用的 VPN 协议，如 PPTP 等，如图 10-87 所示。

(3) 连续单击“下一步”按钮，在“访问规则源”对话框中添加“VPN 客户端”，在“访问规

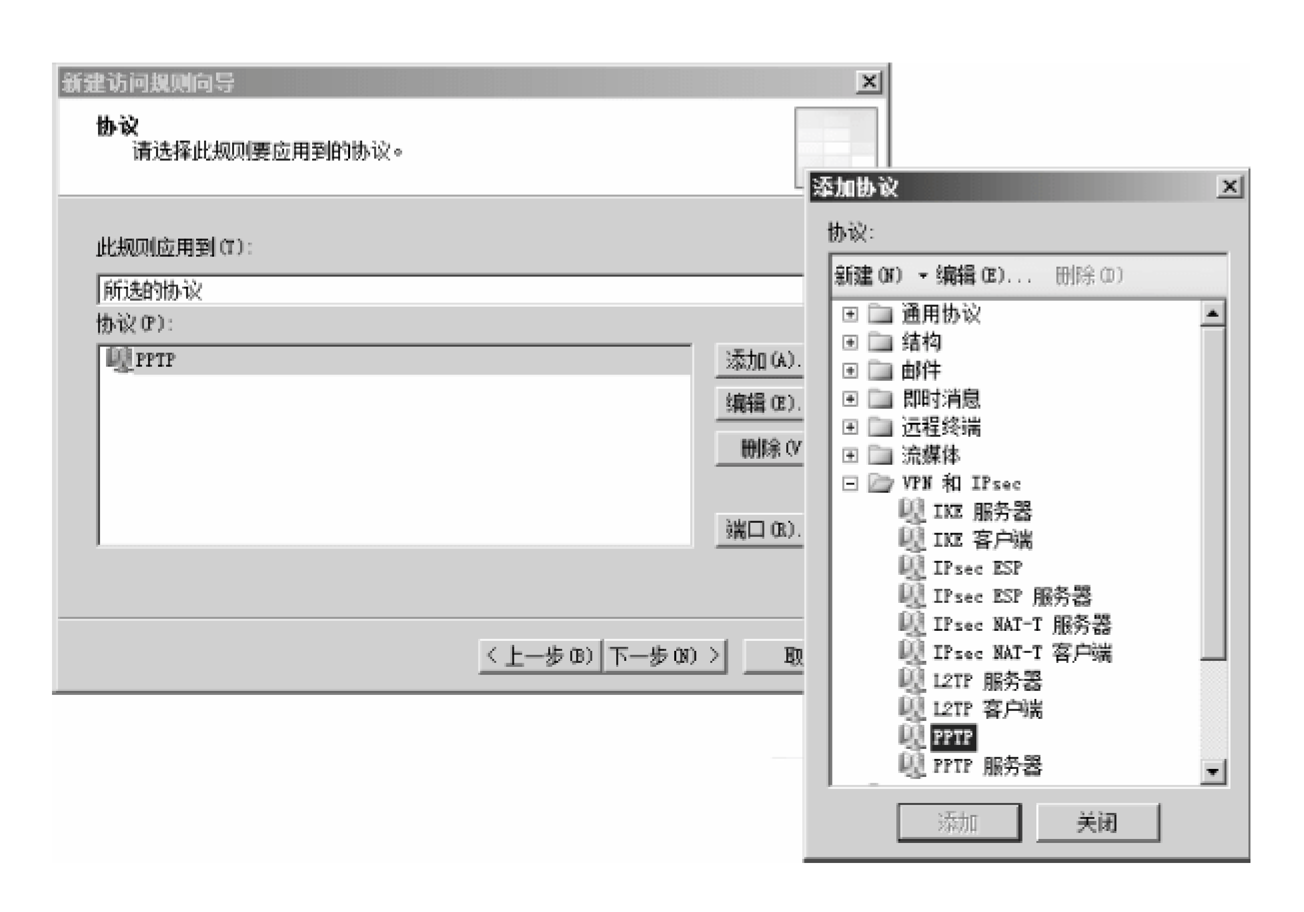


图 10-87　添加 VPN 协议

则目标”对话框中根据需要选择内部、本地主机或者外部。在“恶意软件检查”对话框中，选中“对该规则启用恶意软件检查”单选按钮，如图 10-88 所示。

(4) 单击“下一步”按钮，显示“访问规则源”对话框。单击“添加”按钮，添加“网络”中的“VPN 客户端”选项，如图 10-89 所示。



图 10-88　“恶意软件检查”对话框

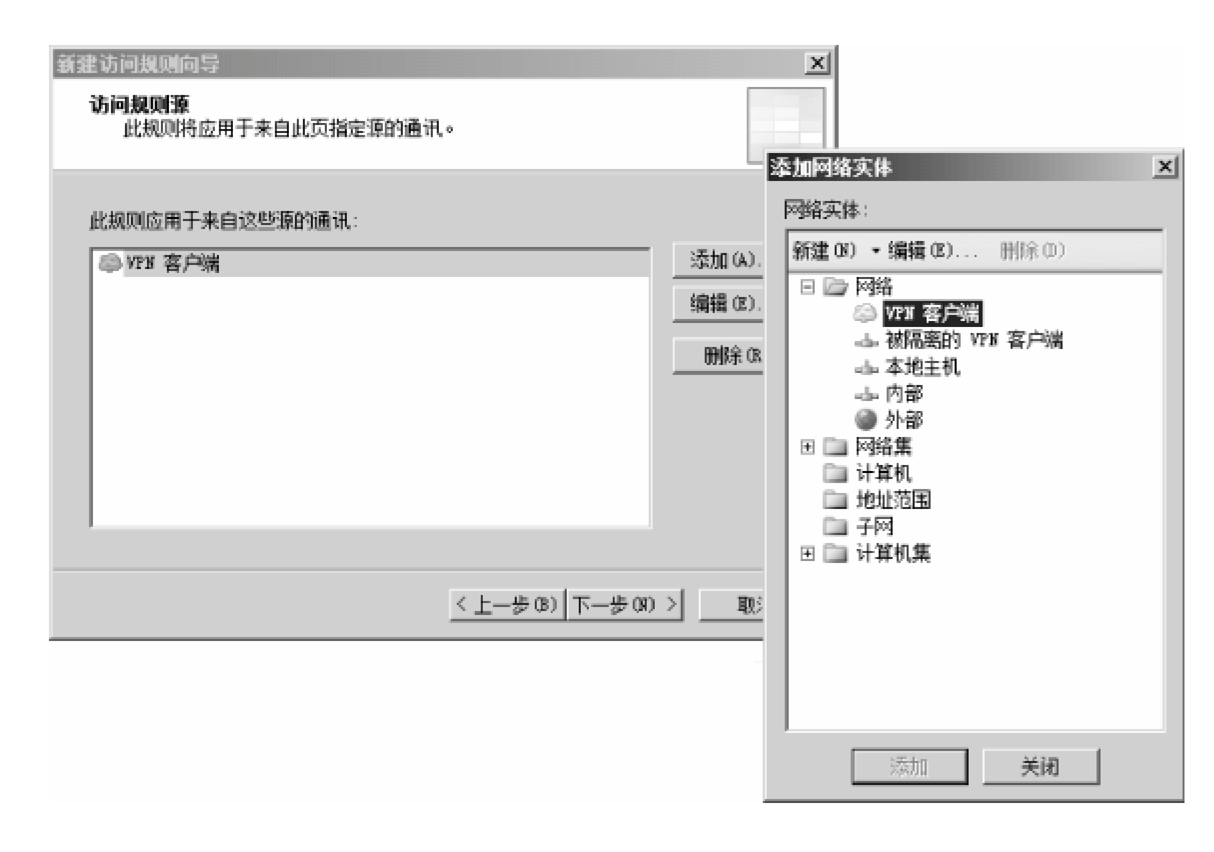


图 10-89　“访问规则源”对话框

(5) 单击“下一步”按钮，显示“访问规则目标”对话框。如果 VPN 服务器是在网络内部，则需单击“添加”按钮，添加“网络”中的“内部”选项，如图 10-90 所示；如果 VPN 服务器安装在当前 TMG 服务器上，则需添加“本地主机”选项。

(6) 依次单击“下一步”按钮，规则创建完成，并单击“应用”按钮，使设置生效即可。

10.5.4　检查 VPN 服务器

在 Forefront TMG 控制台中，配置完 VPN 服务以后，打开“路由和远程访问”控制台，如果“路由和远程访问”已经自动启动(如图 10-91 所示)，则表示 Forefront TMG 上的 VPN 服务器配置完成。否则，就需要启用并配置“路由和远程访问”，启用“VPN 访问”功能，具体操作步骤参见相关内容，这里不再赘述。



图 10-90 “访问规则目标”对话框

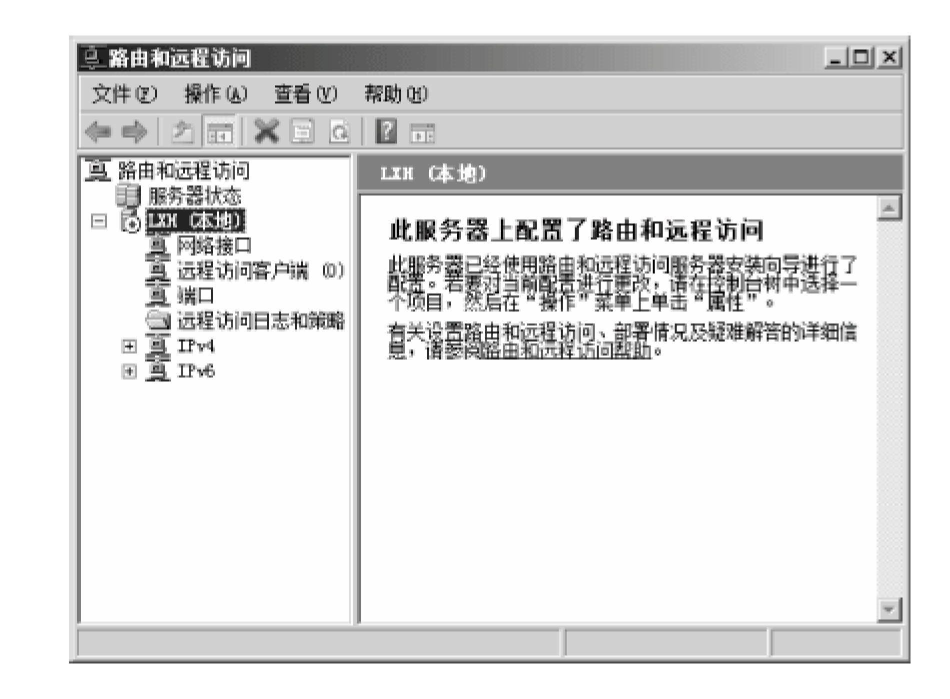


图 10-91 路由和远程访问

习题

1. 什么是 VPN?
2. VPN 有哪些特点?
3. 将一台 Windows Server 2003 服务器配置为 VPN 服务器之前,必须做好哪些准备工作?
4. 简述 SSL VPN 和 IPSec VPN 的区别。
5. 简述 Easy VPN 的定义,主要应用于哪些领域。

实验:借助 Windows Server 2008 实现 VPN

实验目的:

掌握 Windows 环境下 VPN 服务器的搭建、配置和应用。

实验内容:

在 Windows Server 2008 域环境中搭建一台 VPN 服务器,要求使用 RADIUS 身份验证和记账方式。

实验步骤:

(1) 准备用于配置 VPN 服务的计算机,安装双网卡并配置公网 IP 地址。
(2) 启用并配置路由和远程访问中的 VPN 服务。
(3) 设置客户端获取 IP 地址的方式和身份验证方式。
(4) 创建用于远程拨入的域用户账户,并赋予“远程访问”权限。
(5) 分别在 Windows XP 和 Windows Vista 系统环境下,创建 VPN 客户端连接。
(6) 尝试拨入 VPN 服务器所在的专用网,并实现资源共享。

第 11 章 chapter 11

网络访问保护

网络访问安全是目前信息安全领域的一项重要技术，主要包括 Microsoft 推出的 NAP、Cisco 推出的 NAC 和 TCG 组织提出的 TNC 技术。NAP(Network Access Protection，网络访问保护)技术是从 Windows Server 2008 和 Windows Server 2008 R2 系统开始默认集成的，用于为各种网络访问提供安全保护，例如远程桌面访问、VPN 连接等。

11.1 网络访问保护规划

网络攻击并非像想象中的单刀直入，直奔目标而去。因为，可以被定义为攻击目标的服务器或网络设备的安全防御都是非常完善的，甚至无懈可击，只能通过跳板来达到目的，例如网络中某台客户端计算机系统存在的安全漏洞等。目前，该中型企业网络中拥有 500 多台计算机，如果让管理员一一检查每一台计算机是否存在安全漏洞，显然是不现实的，部署 NAP 系统也就成了首选方案。

11.1.1 案例情景

企业网络中的客户端计算机有 500 多台，大部分计算机可以自由访问网络中的共享资源。VPN 拨入用户，可以凭借有效用户账户接入企业内部网络。客户端计算机系统安全性较低，一般只安装了杀毒软件、防火墙中的一种，甚至有些用户“轻装上阵”，没有任何系统安全防御措施。这些计算机一旦连接到局域网，病毒、木马很可能会通过网络袭击局域网中的文件服务器或其他重要计算机，严重时能导致局域网网络发生瘫痪现象。

如今，随着笔记本电脑、PC、手机上网等端点设备的广泛应用，一次不经意的开机或联网，可能已经为整个网络的安全埋下了隐患。不仅如此，该企业网络中对网络设备的接入是未作任何限制的，每个用户都可以将未经统一管理的网络设备连接到网络，进而访问 Internet 与应用程序。不幸的是，企业组织并不能保证这些未经管理的设备与其安全标准兼容，也不能明确第三方的网络访问责任。

企业网络中现有的安全防御措施都是面向客户端的安全软件，例如防病毒系统、防火墙、防间谍软件系统、入侵防御系统等，这些措施虽然可以减轻终端设备的安全防御压力，但其功能通常都是局限于访问权限管理和安全策略部署方面。如果没有网络管理员的配合管理，现有解决方案很难处理网络访问控制方面的难题。

11.1.2 项目需求

在应用 Windows Server 2008 服务器平台之前，网络管理员始终没有找到有效控制危险客户端访问网络的方法。如果使用硬件设备，则无疑会增加企业投资，而经过综合成效和投入的比较，很少企业会采用这种方案。在软件方面，网络访问控制技术的效果的确很难令人满意。自从有了 Windows Server 2008 系统后，这些问题就迎刃而解了，系统自带的 NAP 功能会自动对访问局域网的所有普通计算机强制进行安全检查，如果发现其安全健康标准不达标，则会责令其立即采取安全修正措施，或者干脆禁止其访问局域网网络，这样一来局域网的安全性就能得到有效保证了。

1. 保护漫游计算机的健康

网络中应用笔记本移动办公的用户越来越广泛，例如，需要经常携带笔记本出差的用户，笔记本需要经常连接不安全的外部网络，没有安装更新补丁，没有更新病毒库，或者已经感染病毒，一旦连接到公司网络，需要进行安全检查。

2. 保护桌面计算机的健康

网络中相对比较固定的工作站，虽然可以受到网络防火墙的保护和安全策略限制，但是由于经常接入 Internet，连接移动设备，收发电子邮件等，也可能存在一定的安全隐患，有必要接受补丁包获得更新，并更新病毒库。

3. 保护来访用户计算机的健康

有时候来访用户的计算机需要连接到内部网络，但是，很难保证这些计算机符合网络内部的安全策略，如果强行接入网络，则可能会有安全威胁。此时，可以通过网络访问保护功能在技术层面进行访问限制。当客户计算机连入内部网络之后，NAP 可以将客户计算机重定向到一个隔离的网段，会自动连接到修正服务器，对客户计算机实施制定的安全策略，例如进行自动更新、修复漏洞等，在修复安全之后，客户计算机可以自动连接到内部网络，以上操作自动完成，不耽误业务的进展。

4. 保护家庭计算机的健康

网络中的用户有时候会将工作带到家中处理，需要通过 VPN 等方式将家中的计算机连接到公司内部网络访问资源，此时家中的计算机就有可能对公司内部网络造成安全威胁。使用 NAP 功能可以设置检查家庭计算机，可以将接入的家庭计算机限制到隔离网段，进行健康修复，直到安全为止。

11.1.3 解决方案

该企业网络中大多数客户端计算机系统为 Windows XP 和 Windows Vista，恰恰符合 NAP 客户端的系统需求。综合考虑企业网络环境的现状和用户需求，决定通过部署 NAP 系统，解决网络访问控制方面的难题。

1. 需要部署的 NAP 强制

Windows Vista、Windows XP SP3 和 Windows Server 2008 中的 NAP 支持如下类型的网络访问和通信。

① IPSec 保护通信。

② IEEE 802.1x 身份验证的网络连接。

③ 远程访问 VPN 连接。

④ DHCP 地址配置。

Windows Server 2008 和 Windows Vista 也包含支持连接到 TS 网关服务器的 NAP。管理员可以使用这些类型的网络访问或通信，也叫做 NAP 强制方式，独立或共同限制不符合计算机的访问或通信。

(1) IPSec 强制

使用 IPSec 强制，计算机必须符合使用内网中服务器隔离或域隔离的其他符合计算机初始化的通信，这就要求入站通信受到 IPSec 的保护。因为 IPSec 强制利用 IPSec，用户可以为受保护的通信在每个 IP 或每个 TCP/UDP 端口号上指定要求。IPSec 强制在成功连接和获取有效 IP 地址配置之后，为了符合的计算机限制通信。IPSec 强制是 NAP 中限制网络访问或通信的最强形式之一。

IPSec 组件包括运行 Windows Server 2008 的 HRA 上的 IPSec ES 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 上的 IPSec EC。当 NAP 客户端证明是符合时，HRA 包括基于 X.509 健康证书。当 NAP 客户端使用其他符合的 NAP 客户端初始化 IPSec 保护的通信时，这些健康证书需要与 IPSec 策略设置一同来验证 NAP 客户端。

(2) IEEE 802.1x 强制

使用 IEEE 802.1x 强制，计算机必须可以通过 IEEE 802.1x 身份验证的网络连接来获取不受限的网络访问，网络连接包括认证的以太网交换机或 IEEE 802.1x 无线 AP。对于不符合的计算机，通过以太网交换机或无线 AP 中的受限访问配置文件来限制网络访问。受限访问配置文件可以指定访问控制列表(ACL)，必须符合以太网交换机或无线 AP 上配置的 IP 数据包过滤器的设置，或者符合受限网络 VLAN ID。使用 IEEE 802.1x 强制，健康策略要求在每次计算机尝试 IEEE 802.1x 身份验证网络连接时都要进行强制。IEEE 802.1x 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时应用受限访问配置文件到连接上。

IEEE 802.1x 强制组件包括 Windows Server 2008 中的 NPS 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 上的 EAPHost EC。IEEE 802.1x 为所有通过 IEEE 802.1x 身份验证连接访问网络的计算机，提供强壮的受限网络访问。

(3) VPN 强制

使用 VPN 强制，计算机必须可以通过远程访问 VPN 连接获取不受限的网络访问。对于符合的计算机，通过 VPN 服务器应用在 VPN 连接上的 IP 数据包过滤器的设置来限制网络访问。使用 VPN 强制，健康策略要求在每次计算机尝试获取远程访问 VPN 连接时都要进行强制。VPN 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时为了到 VPN 连接的受限网络访问应用 IP 数据包过滤器。

VPN 强制组件包括 Windows Server 2008 中的 NPS 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 远程访问客户端上的 VPN EC。VPN 强制为所有通过远程访问 VPN 连接访问网络的计算机提供了强壮的受限网络访问。

(4) DHCP 强制

使用 DHCP 强制，计算机必须可以从 DHCP 服务器上获取受限网络访问的 IPv4 地址配置。对于不符合的计算机，网络访问受到 IPv4 地址配置的限制，该配置只允许到受限网

络的访问。使用 DHCP 强制，健康策略要求在每次 DHCP 客户端尝试租借或续借 IPv4 地址配置时都要进行强制。DHCP 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时为只访问受限网络续借 IPv4 地址配置。

DHCP 强制组件包括 Windows Server 2008 DHCP 服务器中的 DHCP ES 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 DHCP 客户端中的 DHCP EC。因为 DHCP 强制依赖于受限 IPv4 地址配置，可以被管理员任意修改，所以该强制是 NAP 中受限网络访问中较弱的形式。

2. NAP 系统的主要组成

图 11-1 显示了启用 NAP 的网络基础结构的组件，启用 NAP 的网络基础结构的组件主要包含以下内容。

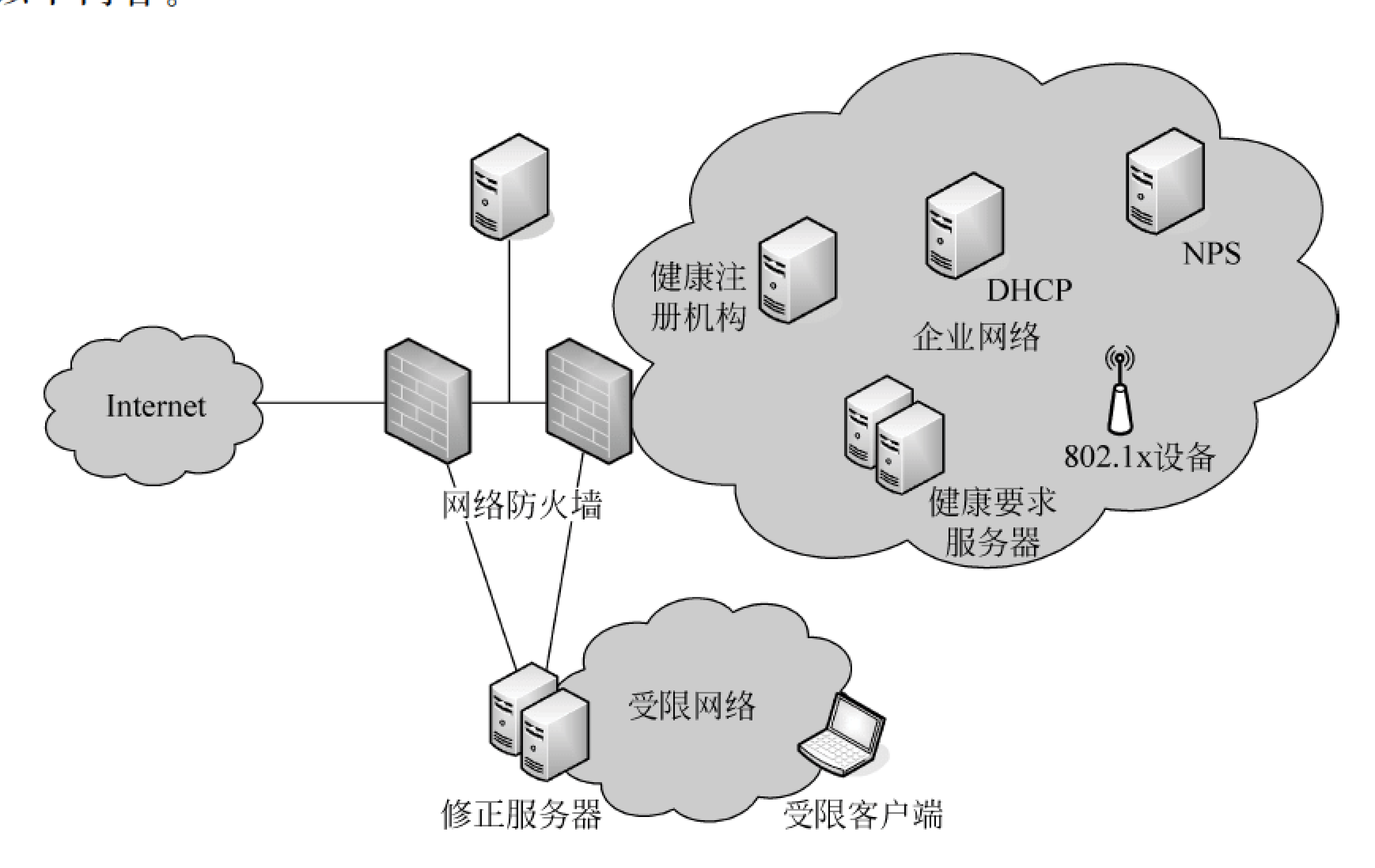


图 11-1　启用 NAP 的网络基础结构

（1）NAP 客户端：支持 NAP 的计算机包括 Windows Server 2008、Windows Vista 或 Windows XP SP3 的计算机。

（2）NAP 强制点：使用 NAP 或可以使用 NAP 的计算机与网络设备要求 NAP 客户端的健康状态评估，并提供受限的网络访问或通信。NAP 强制点使用网络策略服务器（NPS）作为 NAP 健康策略服务器来评估客户端的健康状态信息，网络访问或通信是否被允许，以及不符合的 NAP 客户端必须执行的修正动作的设置。NAP 强制点的示例如下。

① 健康注册机构（HRA）。运行 Windows Server 2008 和 IIS 的计算机，对于符合的 NAP 客户端都具有 CA 颁发的健康证书。

② 网络访问设备。以太网交换机或支持 IEEE 802.1x 身份验证的无线 AP。

③ VPN 服务器。运行 Windows Server 2008 的计算机，以及允许远程访问 VPN 连接内网的路由和远程访问。

④ DHCP 服务器。运行 Windows Server 2008 的计算机，以及提供动态 IPv4 地址配置的 DHCP 服务器服务。

（3）NAP 健康策略服务器：运行 Windows Server 2008 的计算机，以及存储健康要求

策略和提供健康状态验证的 NPS 服务。NPS 代替了 Internet 身份验证服务、RADIUS 服务器和 Windows Server 2003 提供的代理。NPS 也可以作为网络访问的身份验证、授权和记账(AAA)服务器。当作为 AAA 服务器或 NAP 健康策略服务器时,NPS 通常为网络访问和健康要求策略的集中配置使用单独的服务器。NPS 服务也可以运行在基于 Windows Server 2008 的 NAP 强制点上,如 HRA 或 DHCP 服务器。但在这些配置中,NPS 服务是用于 RADIUS 代理与 NAP 健康策略服务器交换 RADIUS 消息的。

(4) 健康要求服务器:为 NAP 健康策略服务器提供当前系统健康状态的计算机。例如,使用杀毒程序的健康要求服务器需要追踪最新版本的病毒库文件。

(5) 活动目录域服务:存储账户证书和属性,以及组策略设置的 Windows 目录服务。虽然不需要健康状态验证,但是活动目录需要 IPSec 保护通信、IEEE 802.1x 验证连接,以及远程访问 VPN 连接。

(6) 受限网络:一个单独的逻辑或物理网络包含以下部分。

① 修正服务器:网络基础结构服务器和 NAP 用来修正不符合状态的健康更新服务器。例如,网络基础结构服务器包括 DNS 服务器和活动目录域控制器。健康更新服务器包括病毒库服务器和软件更新服务器。

② 访问受限的 NAP 客户端:对于不满足健康要求策略的计算机将会被放置在受限网络中。

③ 不支持 NAP 的计算机:不支持 NAP 的计算机将会被放置在受限网络中。

11.2 网络访问保护准备

在网络中部署 NAP 之前,必须对当前网络环境及结构进行合理规划,以便于应用过程中可以根据需要随时加入新的 NAP 应用。必要的准备工作通常包括评价当前的网络基础结构、准备 NAP 组件和搭建所需的网络服务器等。

11.2.1 搭建基础网络环境

在开始 NAP 配置之前,需要详细记录和评价当前网络基础结构,以保证其需要的主机和访问服务器,以及保证其满足支持 NAP 的要求。当前网络基础结构的评价可以分为内网计算机、附属内网的第 2 层和网络支持基础结构。

1. 内网计算机

内网计算机可以分为 NAP 客户端的候选对象和不支持 NAP 的客户端,也可以被分为可管理和不可管理两种。

可管理的计算机主要分为以下两种。

(1) 支持 NAP:运行 Windows Vista、Windows XP SP3 或 Windows Server 2008 的计算机,以及使用 NAP 客户端的其他操作系统。

(2) 不支持 NAP:运行不含有 NAP 客户端的操作系统的计算机。

IEEE 802.1x 和 VPN 的 NAP 强制方式不需要为健康评估管理计算机,但是身份验证和授权计算机则需要被管理。对于 IPSec 的 NAP 强制方式,计算机可以不被管理,但推荐其接受管理。

不可管理的计算机主要分为以下两种。

(1) 支持 NAP：运行 Windows Vista、Windows XP SP3 或 Windows Server 2008 的计算机，以及使用 NAP 客户端的其他操作系统。

(2) 不支持 NAP：运行不含有 NAP 客户端的操作系统的计算机。

2. 域控制器

域控制器的主要功能就是为内网用户和计算机提供基本的身份认证。在网络中部署和应用 NAP 强制之前，首先应在域中创建相应的用户账户或组，例如，NAP 免除安全组、测试用户组等。

NAP 免除安全组用于存储网络中的非 NAP 客户端，如 Windows Server 2003、Windows XP(非 SP3)系统用户等。这些用户无法应用各种 NAP 强制，管理员为符合安全策略和不符合安全策略的客户端设置访问权限后，必须单独为这些客户端指定是授权访问，还是限制访问。

测试用户组则用于存储广泛应用 NAP 强制之前的测试工作。不同的 NAP 强制分别限制不同类型的网络访问。如果由于应用了网络健康评估策略，而影响了正常的网络应用，就得不偿失了。因此，应用 NAP 强制之前必须在小范围内进行测试。

3. 证书服务器

数字证书是最常用的网络安全保护手段之一。在部署 NAP 强制的网络中，证书服务器的主要作用，就是为网络中的各种服务器角色或客户端颁发数字证书，实现彼此之间的身份验证。证书服务器在 IPSec 强制的网络中是必需的，而在其他 NAP 强制的网络中则是可选的。例如，在 VPN 强制网络中，如果用户选择了特定的加密传输协议和身份验证方式，则可能需要准备数字证书，验证 VPN 服务器和 VPN 客户端身份的有效性。

4. 网络策略服务器

网络策略服务器(NPS)是任何 NAP 强制都必需的，提供各种安全健康评估、记账等功能，是 Windows Server 2008 系统的新增功能之一。NPS 允许用户通过 RADIUS 服务器、RADIUS 代理和网络访问保护策略服务器，集中配置和管理网络策略。

(1) RADIUS 服务器

从 Windows Server 2008 系统开始，RADIUS 服务器已经被集成在 NPS 中。作为 RADIUS 服务器，NPS 为许多类型的网络访问(包括无线、身份验证切换、VPN 远程访问，路由器到路由器的连接)执行集中化的连接身份验证、授权和记账。

RADIUS 服务器具有对用户账户信息的访问权限，并可以检查网络访问身份验证凭据。如果用户的凭据是真实的，并且连接尝试获得授权，RADIUS 服务器将根据指定条件向用户授予访问权限，并将网络访问连接记录到记账日志中。使用 RADIUS 允许在一个中心位置(而不是在每台访问服务器上)收集并维护网络访问用户身份验证、授权和记账数据。

(2) RADIUS 代理

作为 RADIUS 代理，NPS 将身份验证和记账消息转发到其他 RADIUS 服务器。使用 NPS，各组织还可以在保留对用户身份验证、授权和记账活动控制的同时，将远程访问基础结构外包给服务提供商。

(3) NAP 策略服务器

NAP 包含在 Windows Vista 和 Windows Server 2008 中，并通过确保按照组织网络健

康策略配置客户端计算机后才允许其连接到网络资源,从而有助于保护对专用网络的访问。此外,计算机连接到网络时,NAP 会监视客户端计算机对管理员定义的健康策略的遵从性情况。使用 NAP 自动更新,可以自动更新不符合要求的计算机,以使其遵从健康策略,从而使它们能够连接到网络。

系统管理员可以定义网络健康策略,并使用 NPS 中或其他公司(取决于 NAP 部署)提供的 NAP 组件创建这些策略。

健康策略可以包含软件要求、安全更新要求和所需的配置设置等内容。NAP 通过检查和评估客户端计算机的健康,在认为客户端计算机不健康时限制网络访问以及修正不健康的客户端计算机以进行充分的网络访问,来强制运行健康策略。

5. 更新服务器

当用户配置健康要求策略来强制受限访问时,更新服务器是不符合的 NAP 客户端可以访问的内网的子集。更新服务器包括网络基础结构服务器和健康更新服务器。不符合的 NAP 客户端,使用这些服务器或服务器上的资源来自动或手动执行更新。健康要求策略也可以为不支持 NAP 的客户端强制受限访问。

如果使用报告模式,则不需要更新服务器。在报告模式下,不符合的 NAP 客户端的访问不受限制。但是,为了避免不符合健康要求的计算机为内网带来的威胁,必须最终转换到强制模式,即需要建立更新服务器。

在 VPN 和 DHCP 模式下不符合的 NAP 客户端,可以访问的更新服务器列表,需要与 NAP 客户端健康评估匹配的网络策略的 NAP 强制设置中,指定的更新服务器组相符合。更新服务器组是一个 IPv4 地址和 IPv6 地址的列表。该列表应该包括网络基础结构服务器和健康更新服务器。

基础结构服务器包括以下部分。

(1) DHCP 服务器:为不符合的 NAP 客户端分配 IPv4 地址和其他配置参数,保证其可以访问更新服务器。如果用户正使用 DHCP 强制方式,则不需要添加支持 NAP 的 DHCP 服务器作为更新服务器。

(2) DNS 服务器和 WINS 服务器:为不符合的 NAP 客户端提供名称解析,保证其可以解析名称,并访问其他更新服务器。

(3) 活动目录域控制器:保证不符合的 NAP 客户端可以执行域登录,访问基于域的资源,如文件共享。

(4) Internet 代理服务器:保证不符合的 NAP 客户端可以访问 Internet。

(5) HRA:保证不符合的 NAP 客户端可以在 IPSec 强制模式下获取健康证书。

更新 NAP 客户端系统健康需要健康更新服务器,包括以下部分。

(1) 疑难解答 URL 服务器:在"更新服务器和疑难解答 URL"对话框的疑难解答 URL 文本框中,指定 Web 服务器。

(2) 反病毒更新服务器:这些服务器可能位于 Internet 上。如果用户拥有 Internet 代理服务器作为更新服务器,则不需要包含基于 Internet 的反病毒更新服务器。如果在内网中拥有反病毒更新服务器,则应该将其作为更新服务器,因为在尝试连接访问基于 Internet 的反病毒服务器前,通常会首先在这些服务器上检查更新。

(3) 反间谍更新服务器:如同反病毒服务器一样,如果在内网中配置了反间谍更新服

务器,则需将其作为更新服务器。如果只存在于 Internet 上,确保 Internet 代理服务器包含在更新服务器组中。

(4) 软件更新服务器:如同反病毒服务器一样,如果在内网中配置了软件更新服务器,则需将其作为更新服务器。如果只存在于 Internet 上,确保 Internet 代理服务器包含在更新服务器组中。

更新 NAP 客户端所需要的健康更新服务器的设置依赖于用于健康评估的 SHV。

11.2.2 安装 NPS

在 Active Directory 环境中部署 NAP 系统,用户可以更充分地使用其提供的网络访问保护功能。客户端可以是 Windows Server 2008、Windows Vista 或 Windows XP SP3 系统,同时确保已加入域。默认安装完成 Windows Server 2008 后,没有安装网络策略和远程访问服务,需要网络用户手动安装该服务。

(1) 运行"添加角色向导",在"选择服务器角色"对话框中,选中"网络策略和访问服务"复选框,如图 11-2 所示。



图 11-2 "选择服务器角色"对话框

(2) 单击"下一步"按钮,显示"网络策略和访问服务"对话框。其中概要介绍了"网络策略和访问服务"完成的功能,单击"其他信息"中的链接可以查看详细帮助文件。单击"下一步"按钮,显示如图 11-3 所示的"选择角色服务"对话框。在"角色服务"列表中,选中"网络策略服务器"复选框。

提示: 本文中设计的案例只是网络访问保护系统的一个简单应用,适用于大多数网络环境。角色服务中的"路由和远程访问服务"、"健康注册机构"和"主机凭据授权协议"只有在特殊环境中才会用到,这里不作选择。需要注意的是,选择这些角色后,需要添加相应的角色服务和功能组件,如选择"健康注册机构"角色,就需要安装 Active Directory 证书服务、Web 服务器等。

(3) 单击"下一步"按钮,显示"确认安装选择"对话框。其中列出了已选择安装的服务设置信息。单击"安装"按钮,开始安装选择的服务。安装完成后,显示如图 11-4 所示的"安装结果"对话框。



图 11-3 “选择角色服务”对话框



图 11-4 “安装结果”对话框

(4) 单击“关闭”按钮，完成“网络策略和访问服务”的安装。

11.2.3 配置 NAP 向导

初级用户可以通过配置 NAP 向导，快速部署希望实施的 NAP 强制。如果对 NAP 运行机制比较熟悉，则用户也可以通过直接配置相关 NAP 强制所需的策略，来达到实施 NAP 强制的目的，主要包括连接请求策略、网络策略和健康策略。在运行配置 NAP 向导的过程中，将自动生成相应的策略。

依次选择“开始”→“管理工具”→“网络策略服务器”选项，显示如图 11-5 所示的“网络策略服务器”窗口。在右侧下拉列表框中，选择“网络访问保护(NAP)”选项。

单击“配置 NAP”按钮，显示如图 11-6 所示的“选择与 NAP 一起使用的网络连接方法”对话框。根据需要在下拉列表框中，选择网络连接方式(NAP 强制方式)，系统会自动为



图 11-5 “网络策略服务器”窗口



图 11-6 “选择与 NAP 一起使用的网络连接方法”对话框

NAP 健康要求策略创建一个名称,也可根据需要进行修改。接下来的操作依据所选网络连接方法的不同,配置过程也会有所不同,详细操作步骤参考本章后续内容的介绍。

11.2.4 配置更新服务器

实施 NAP 强制的关键目的并不是绝对禁止非 NAP 客户端或存在安全风险的 NAP 客户端访问内部网络,而是如何帮助这些客户端安全地接入网络,访问所需资源。更新服务的功能就是帮助不符合策略要求的 NAP 客户端完善系统安全配置,如提供 Windows Update、防病毒程序更新等。NAP 系统中所需的更新服务器必须在准备工作中一一部署,在 NPS 服务器上只需创建这些服务器的分组列表即可。

在“网络策略服务器”控制台中,展开“网络访问保护”节点,右击“更新服务器组”并在弹出的快捷菜单中选择“新建”选项。在出现的“新建更新服务器组”对话框中,可以通过 DNS 名称、IPv4 地址或 IPv6 地址指定更新服务器,如图 11-7 所示。

单击“添加”按钮，显示如图 11-8 所示的“添加新服务器”对话框，在“友好名称”文本框中输入便于识别的服务器名称，在“IP 地址或 DNS 名称”文本框中输入企业网络提供指定功能的服务器名称或 IP 地址。最后，单击“确定”按钮，将其添加到新建更新服务器组中即可。按照这种方法可以向统一更新服务器组中添加多台更新服务器，并可以配置多个更新服务器组。

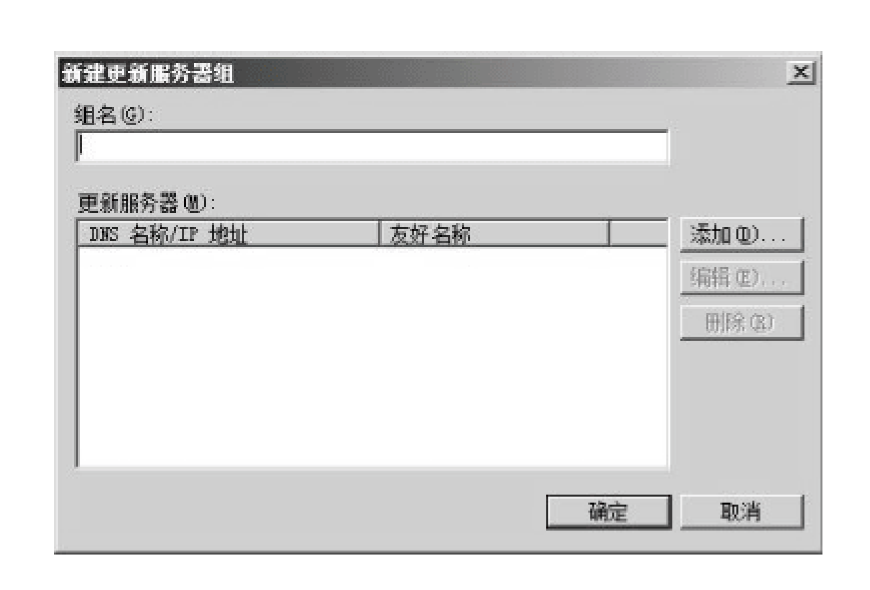


图 11-7 “新建更新服务器组”对话框

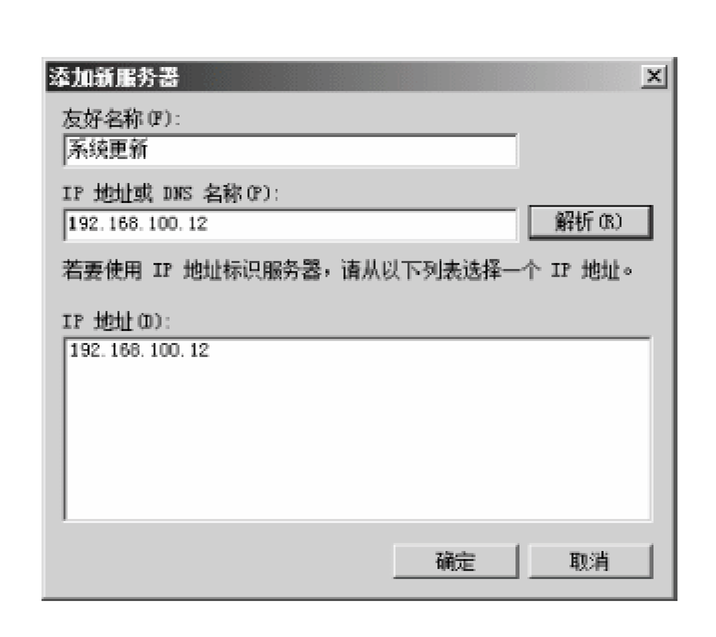


图 11-8 “添加新服务器”对话框

11.3 配置 IPSec 强制

IPSec 本身就是一种基于 IP 的通信安全保障机制。通过在企业网络的部分客户端或服务器之间启用 IPSec，可以大大提升网络通信的安全性和可靠性。而 NAP 系统的 IPSec 强制则是在此基础上，增加了验证通信双方系统健康评估环节，避免安全风险的扩散。只有通过 NPS 服务器的健康策略评估，获得健康认证证书，客户端计算机才能建立到其他计算机或服务器的 IPSec 连接。

11.3.1 配置 PKI

为 IPSec 强制配置基于 Windows 的 PKI，需要完成以下工作。

① 添加根 CA(根据需要)。

② 在发布 CA 级别创建 NAP CA。

③ 验证 NAP CA 的属性(企业 CA)。

④ 为健康证书创建证书模板(企业 CA)。

⑤ 配置 NAP CA 允许非默认的生命周期(企业 CA)。

⑥ 配置健康证书模板的自动注册(企业 CA)。

⑦ 为健康证书公布证书模板(企业 CA)。

⑧ 配置证书的自动注册。

1. 添加根 CA

如果用户没有基于 Windows 的 PKI，则必须在安全网络中的计算机上创建根 CA，根据企业需要和安全策略创建中间一级的 CA。

2. 在发布 CA 级别创建 NAP CA

为了在运行 Windows Server 2008 的计算机上添加 NAP CA，使用“服务器管理器”，安装“Active Directory 证书服务”角色。对于 NAP CA，不需要证书颁发机构 Web 自动注册、

联机应答，或网络设备自动注册服务角色。在安装活动目录证书服务角色的过程中，如果NAP客户端没有使用HRA的DNS发现，保证NAP CA计算机作为证书层级的发布CA中的从属、独立的CA，此时，保证NAP CA计算机是从属的企业CA。

3. 验证NAP CA的属性

必须验证NAP CA不需要管理员批准要求的证书，具体操作步骤如下。

（1）依次选择“开始”→“管理工具”→“证书颁发机构”选项，显示如图11-9所示的“certsrv-[证书颁发机构(本地)]”窗口。

（2）右击NAP CA的名称并在快捷菜单中选择“属性”选项，显示“coolpen-AD1-CA 属性”对话框，切换到如图11-10所示的“策略模块”选项卡。

图11-9　“certsrv-[证书颁发机构(本地)]”窗口

（3）单击“属性”按钮，显示如图11-11所示的“属性”对话框。在“请求处理”选项卡中，选中“如果可以的话，按照证书模板中的设置。否则，将自动颁发证书。”单选按钮。

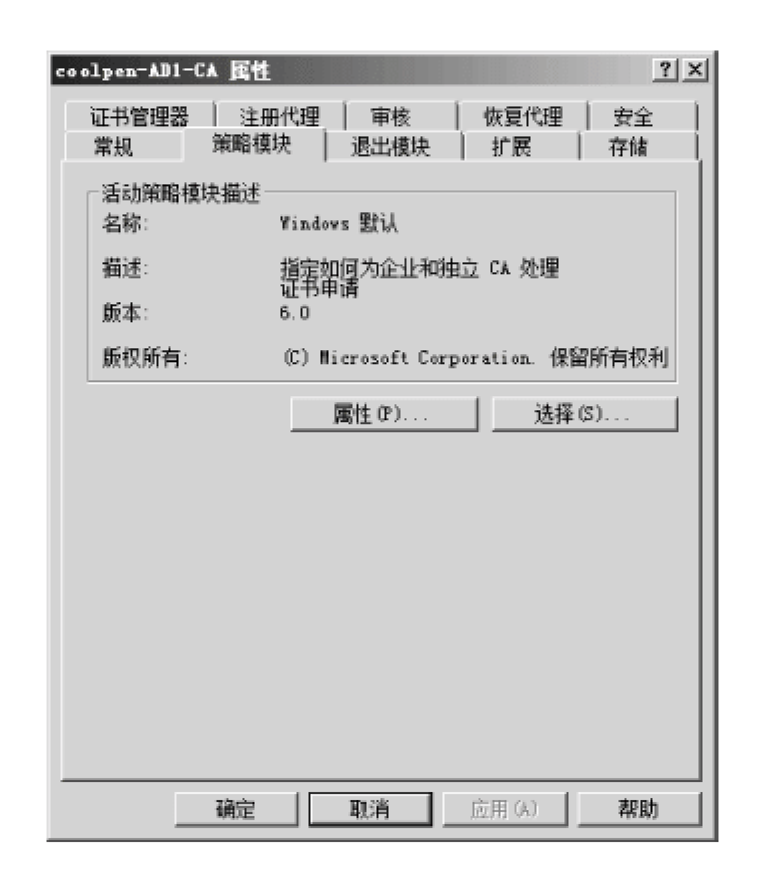


图11-10　“策略模块”选项卡

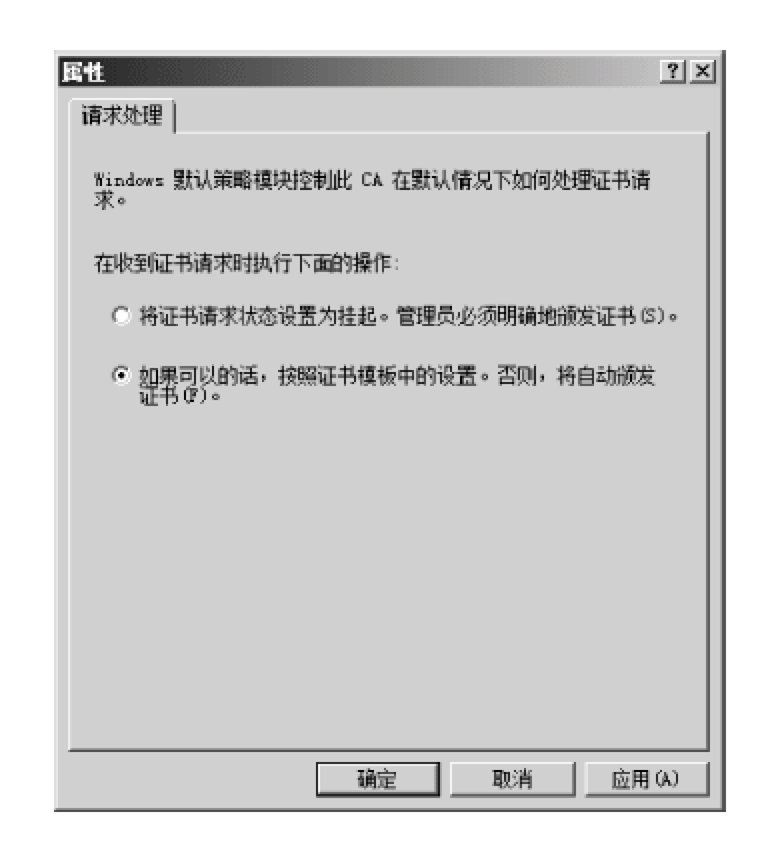


图11-11　“属性”对话框

（4）连续单击“确定”按钮，保存设置。

4. 为健康证书创建证书模板

对于基于Windows Server 2003的NAP CA，必须手动创建系统健康身份验证证书模板，保证IPSec安全组的成员可以自动注册长生命周期的健康证书。对于基于Windows Server 2008的NAP CA，系统中已经包括了系统健康身份验证证书模板，但是，必须确保系统健康身份验证证书模板拥有适当的自动注册的权限。

（1）依次选择“开始”→“运行”选项，在“打开”文本框中输入certtmpl.msc，按Enter键运行，显示如图11-12所示的“证书模板控制台”窗口。

（2）右击“工作站身份验证”并在快捷菜单中选择“复制模板”选项，显示如图11-13所示的“复制模板”对话框，设置模板最低支持的操作系统版本，建议选中Windows Server 2003 Enterprise单选按钮，以便可以将创建后的模板应用到运行Windows Server 2003系统的证书服务器上。



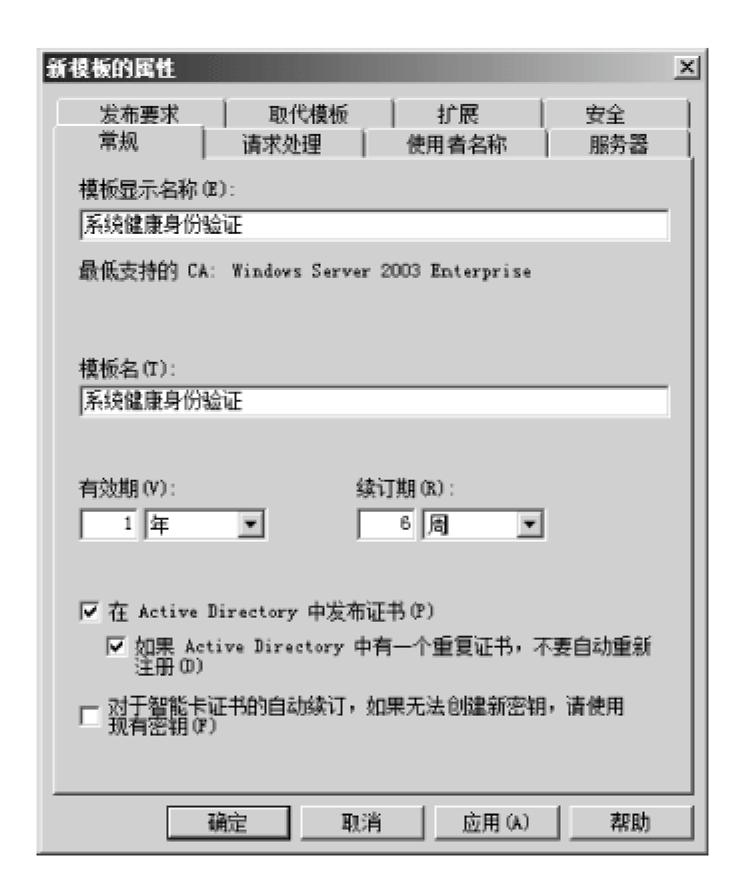




图 11-12 “证书模板控制台”窗口　　　　图 11-13 “复制模板”对话框

(3) 单击“确定”按钮，显示如图 11-14 所示的“新模板的属性”对话框。在“模板显示名称”文本框中，输入“系统健康身份验证”。选中“在 Active Directory 中发布证书”复选框，使该证书在域环境中颁发。

(4) 切换到“扩展”选项卡，在“这个模板中包括的扩展”列表中，选择“应用程序策略”选项。单击“编辑”按钮，显示如图 11-15 所示的“编辑应用程序策略扩展”对话框。



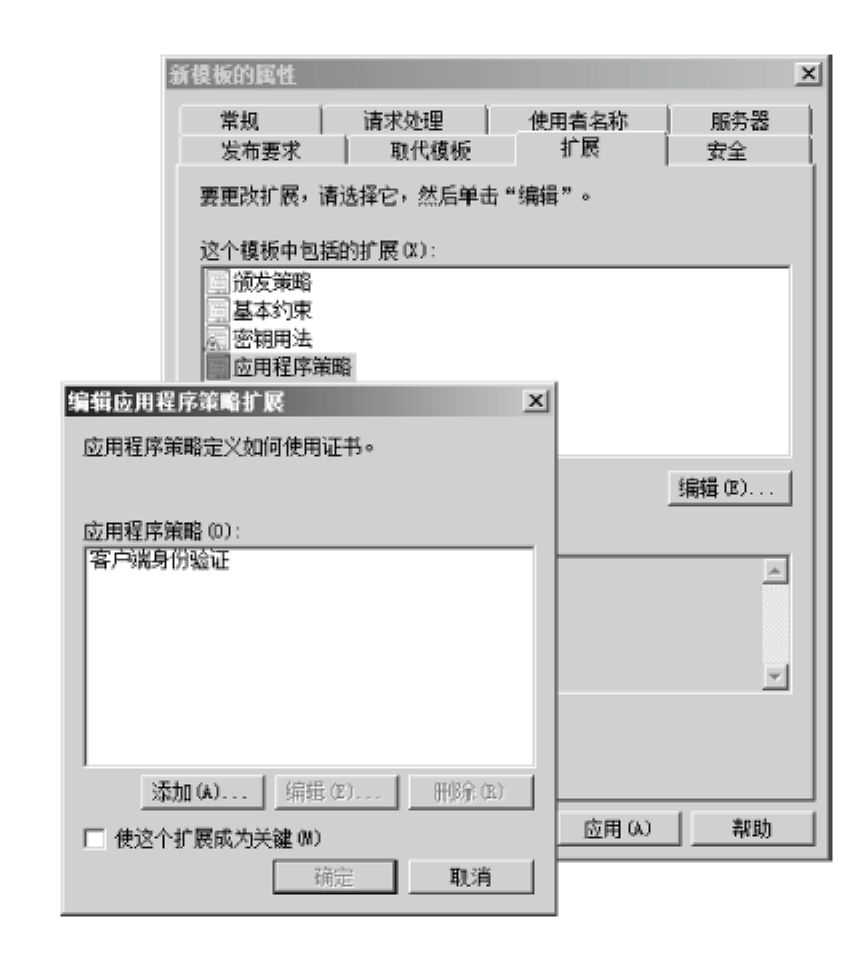


图 11-14 “新模板的属性”对话框　　　　图 11-15 “编辑应用程序策略扩展”对话框

(5) 单击“添加”按钮，显示如图 11-16 所示的“添加应用程序策略”对话框。在“应用程序策略”列表中，选择“系统健康身份验证”选项。

(6) 连续单击“确定”按钮，返回“新模板的属性”对话框，切换到如图 11-17 所示的“安全”选项卡，确保 Authenticated Users 组拥有“读取”权限即可。

(7) 单击“添加”按钮，显示如图 11-18 所示的“选择用户、计算机、服务账户或组”对话框，输入 IPSec NAP 安全组的名称，单击“检查名称”按钮，检查输入的组名是否正确。

(8) 单击“确定”按钮，在“安全”选项卡中，选择 IPSec NAP 安全组的名称，在“IPSec 的权限”列表中选择“注册”和“自动注册”对应的“允许”复选框，如图 11-19 所示。



图 11-16　“添加应用程序策略”对话框



图 11-17　“安全”选项卡

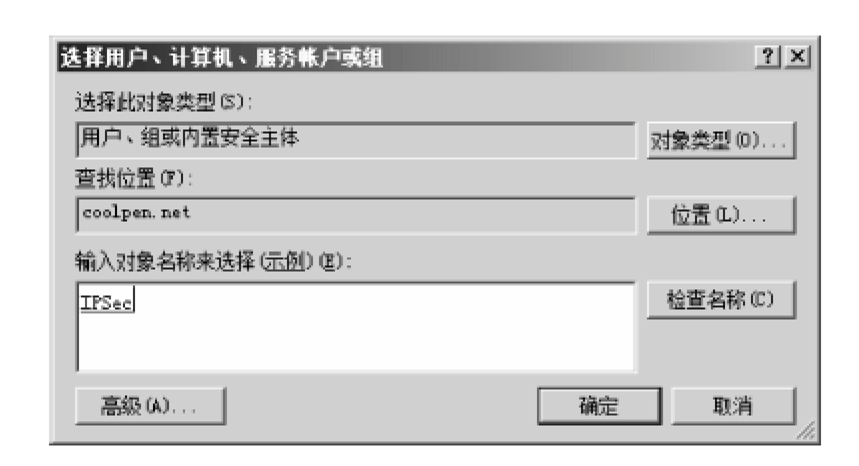


图 11-18　“选择用户、计算机、服务账户或组”对话框

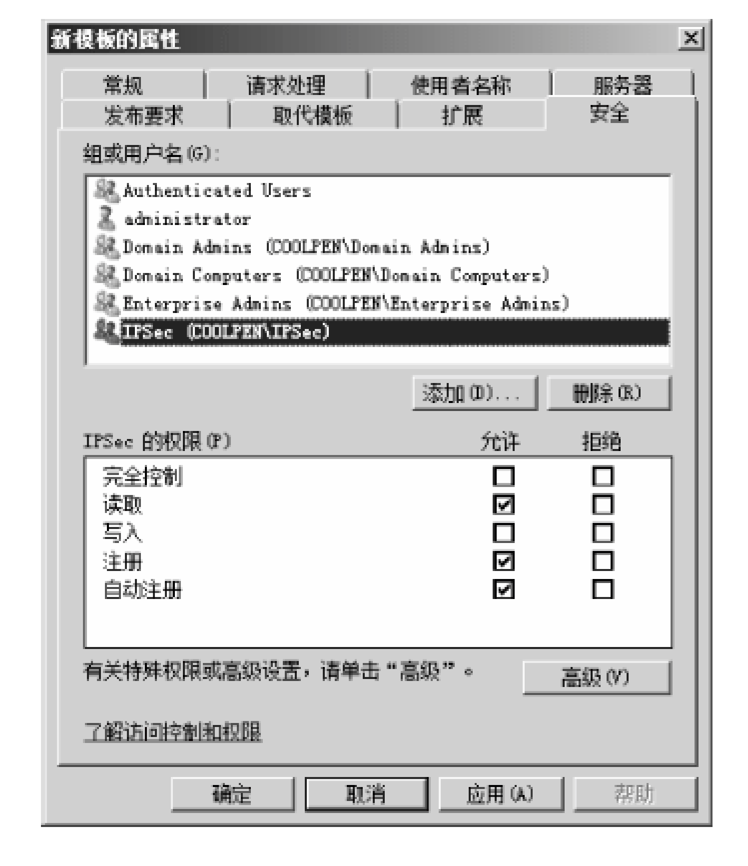


图 11-19　赋予 IPSec 安全组权限

（9）单击“确定”按钮，保存设置。此时，新模板即可添加到模板控制台中，如图 11-20 所示。

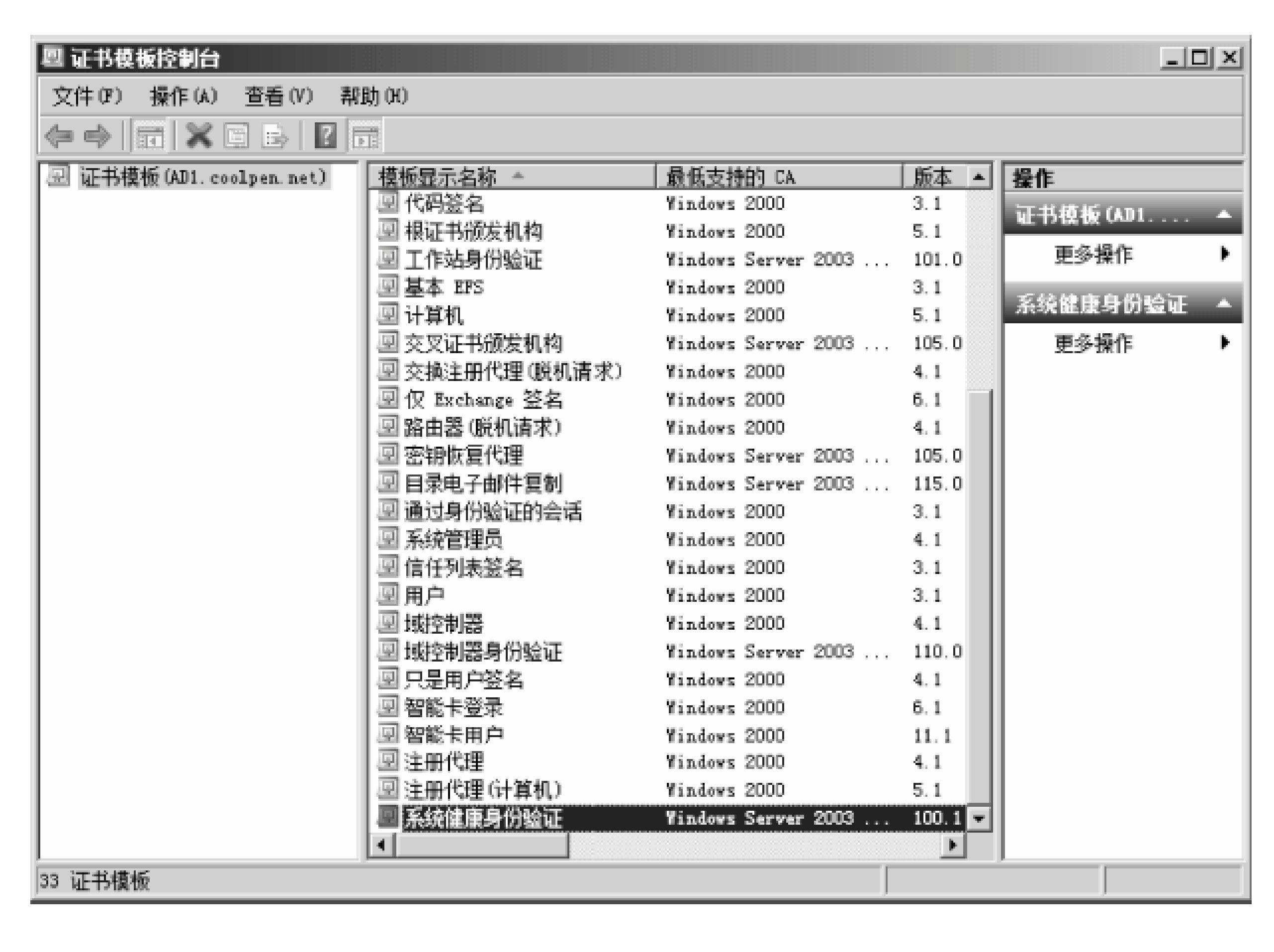


图 11-20　成功创建模板

5. 发布新的健康证书模板

(1) 在根 CA 计算机上，运行"证书颁发机构"管理单元，右击"证书模板"，在快捷菜单中依次选择"新建"→"要颁发的证书模板"选项，显示如图 11-21 所示的"启用证书模板"对话框。

(2) 选中"系统健康身份验证"，单击"确定"按钮，即可颁发该模板，如图 11-22 所示。

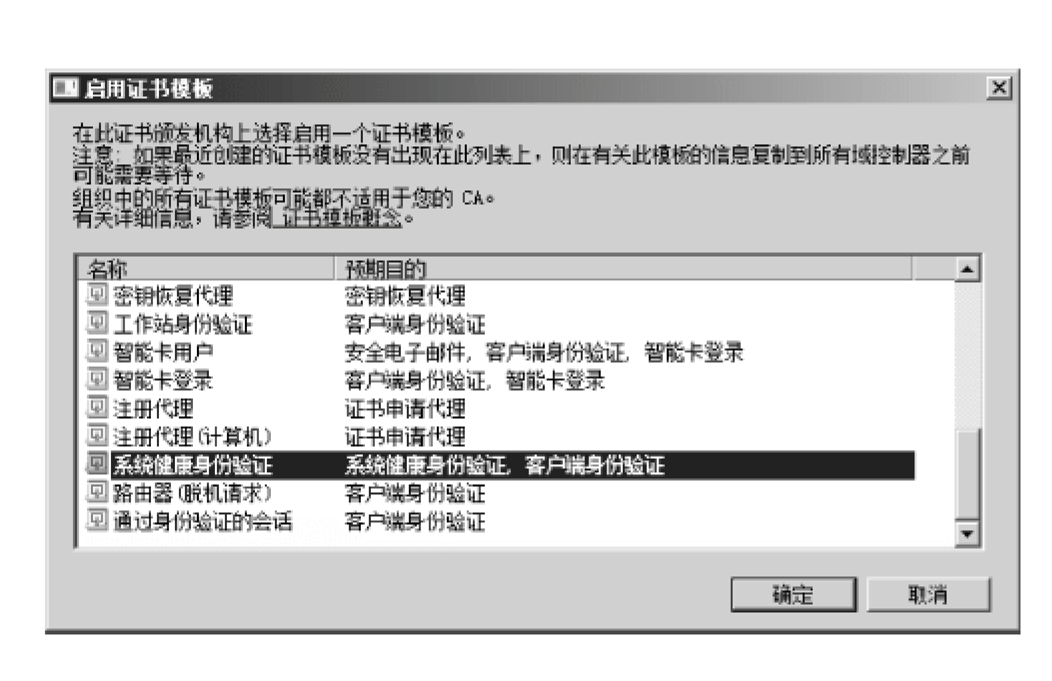




图 11-21 "启用证书模板"对话框

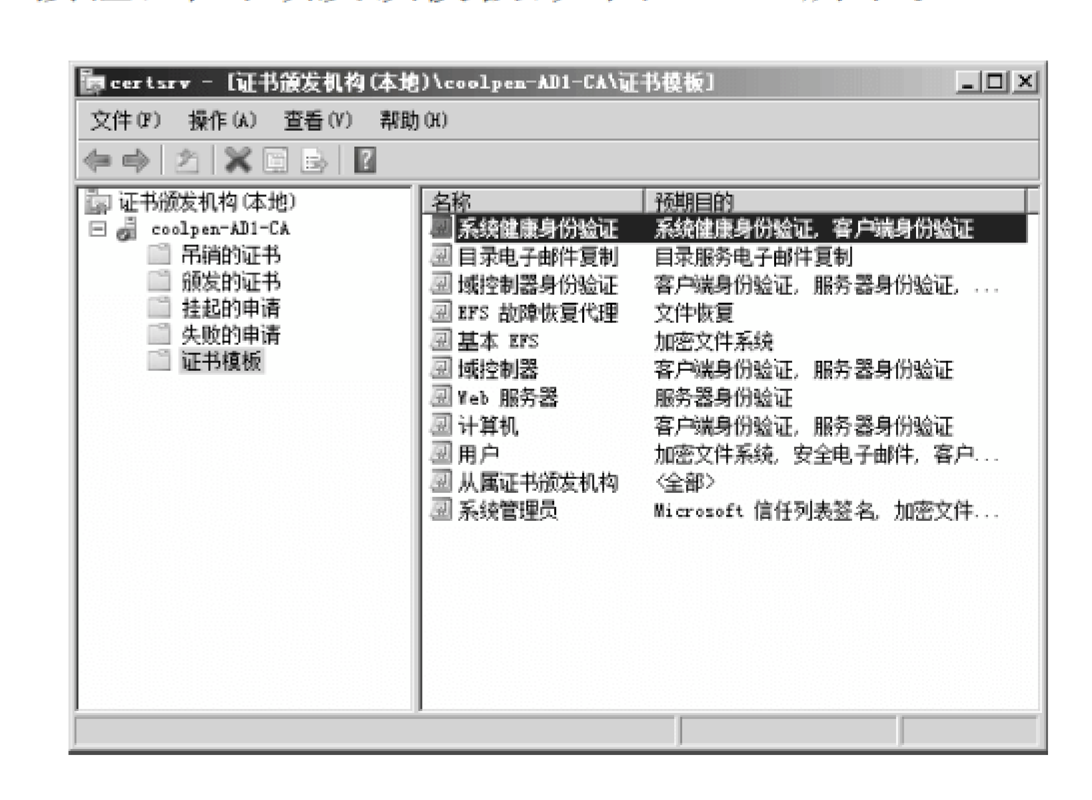


图 11-22 成功发布新的模板

6. 配置 NAP CA 允许非默认的生命周期

企业 NAP CA 必须配置为允许非默认的生命周期。否则，符合的 NAP 客户端将被发布健康证书模板指定的生命周期的健康证书，而不是 HRA 配置中指定的短生命周期。

配置企业 NAP CA 允许非默认的生命周期的具体操作步骤如下。

(1) 在企业 NAP CA 计算机的命令行提示符窗口中，运行如下命令，显示如图 11-23 所示结果。

```
certutil.exe -setreg policy\EditFlags +EDITF_ATTRIBUTEENDDATE
```

```
管理员: 命令提示符
C:\Users\administrator.COOLPEN>certutil.exe -setreg policy\EditFlags +EDITF_ATTR
IBUTEENDDATE
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\coolpen-LXH-CA\PolicyMod
ules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

旧值:
  EditFlags REG_DWORD = 11014e (1114446)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

新值:
  EditFlags REG_DWORD = 11016e (1114478)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_ATTRIBUTEENDDATE -- 20 (32)
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -setreg 命令成功完成。
CertSvc 服务可能需要重新启动，以使更改生效。

C:\Users\administrator.COOLPEN>
```

图 11-23 配置企业 NAP CA

(2) 运行 net stop certsvc 和 net start certsvc 命令，重启活动目录证书服务，如图 11-24 所示。

7. 配置健康证书模板的自动注册

为了使边界计算机(IPSec NAP 安全组成员)自动获取长生命周期的健康证书,必须在活动目录中启用证书自动注册。

在"组策略管理编辑器"窗口中,依次展开"计算机配置"→"策略"→"Windows 设置"→"安全设置"→"公钥策略"选项。双击"证书服务客户端-自动注册",显示如图 11-25 所示的"证书服务客户端-自动注册 属性"对话框。在"配置型号"下拉列表框中,选择"已启用"选项,并选中"续订过期证书、更新未决证书并删除吊销的证书"和"更新使用证书模板的证书"复选框。单击"确定"按钮,保存设置即可。



图 11-24 重启 Active Directory 证书服务

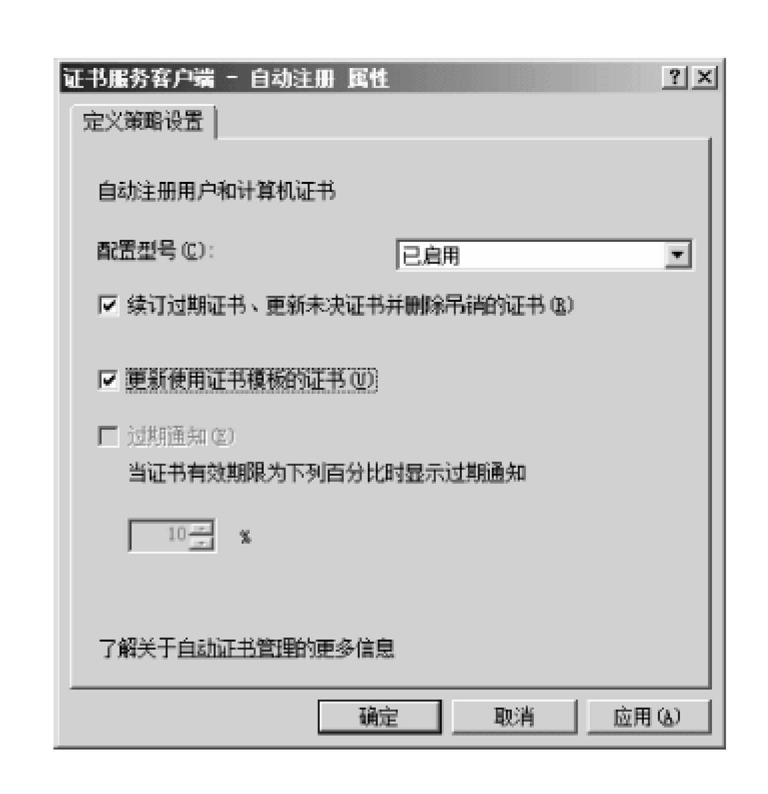


图 11-25 "证书服务客户端-自动注册 属性"对话框

11.3.2 配置 HRA

配置 HRA 主要包括添加 HRA 到 IPSec NAP 安全组、安装计算机证书、配置网络策略和访问服务角色、使用 HRA 权限配置 NAP CA、配置 HRA 的属性、为 RADIUS 代理在 HRA 上配置 NPS 服务和为 SSL 配置 IIS。

1. 添加 HRA 到 IPSec NAP 安全组

HRA 计算机账户必须是 IPSec NAP 安全组中的成员,以保证其立即拥有一个长期的健康证书,允许其与安全网络中的计算机通信。添加 HRA 计算机账户到 IPSec NAP 安全组中。

(1) 在"活动目录用户和计算机"窗口中,双击 IPSec NAP 安全组的名称,显示如图 11-26 所示的"IPSec 属性"对话框。

(2) 切换到"成员"选项卡,单击"添加"按钮,显示"选择用户、联系人、计算机或组"对话框。单击"对象类型"按钮,显示如图 11-27 所示的"对象类型"对话框,选中"计算机"复选框。

(3) 单击"确定"按钮,返回"选择用户、联系人、计算机或组"对话框。在"输入对象名称来选择"文本框中,输入 HRA 计算机的名称,单击"检查对象"按钮,检查输入的计算机是否正确。



图 11-26 "IPSec 属性"对话框

（4）连续单击“确定”按钮，保存设置即可。

2. 使用 HRA 权限配置 NAP CA

NAP CA 必须配置允许 HRA 组件请求证书的权限，HRA 计算机也可以被授予管理 CA 的权限，以保证其可以从 NAP CA 证书数据库中自动删除过期的证书。

（1）在“证书颁发机构”管理单元，右击 NAP CA 的名称，在快捷菜单中选择“属性”选项，打开“coolpen-LXH-CA 属性”对话框，并切换到“安全”选项卡。

（2）单击“添加”按钮，打开“选择用户、联系人、计算机或组”对话框。单击“对象类型”按钮，显示如图 11-28 所示的“对象类型”对话框，选中“计算机”复选框。

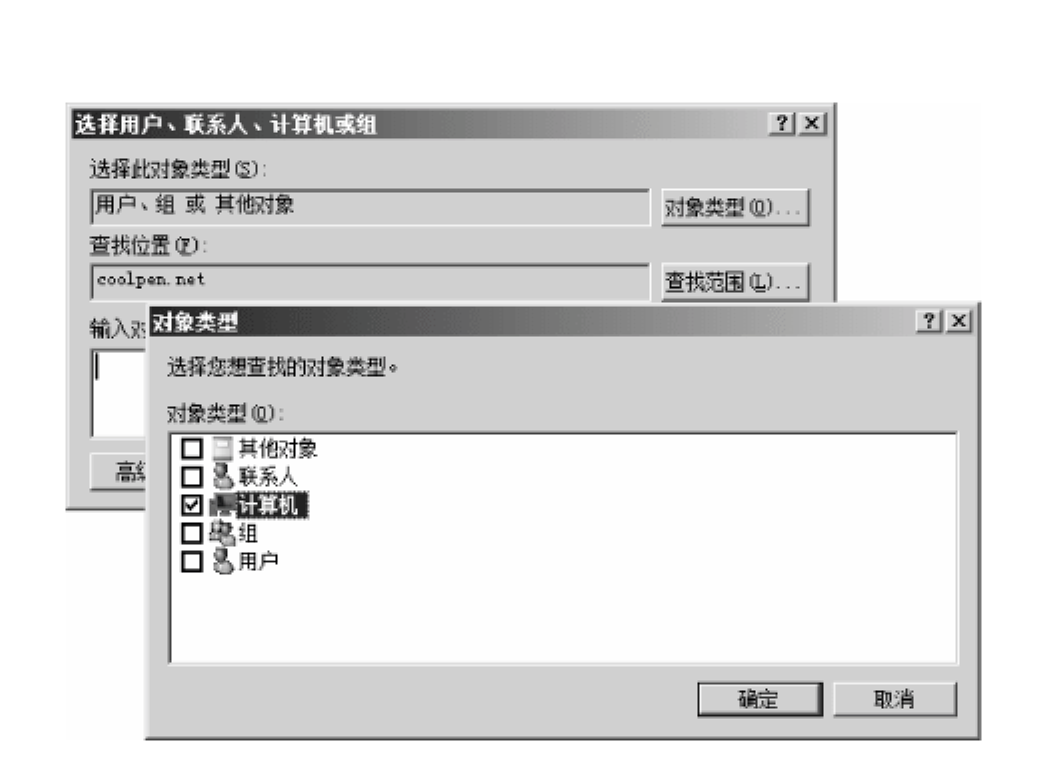


图 11-27 “对象类型”对话框(1)



图 11-28 “对象类型”对话框(2)

（3）单击“确定”按钮，返回“选择用户、联系人、计算机或组”对话框。在“输入对象名称来选择”文本框中，输入 HRA 计算机的名称，单击“检查对象”按钮，检查输入的计算机名是否正确。

（4）单击“确定”按钮，返回“安全”选项卡。在“组或用户名”列表中，选择 HRA 计算机的名称，然后在权限列表中选中“颁发和管理证书”和“请求证书”复选框。如果使用自动 CA 数据库管理，则需要选中“管理 CA”复选框，如图 11-29 所示。

（5）单击“确定”按钮，保存设置，并关闭该属性对话框。

3. 配置 HRA 的属性

（1）在安装 HRA 的计算机上，依次选择“开始”→“管理工具”→“健康注册结构”选项，打开如图 11-30 所示的“健康注册机构(本地计算机)”窗口。

（2）右击“证书颁发机构”并选择快捷菜单中的“属性”选项，显示如图 11-31 所示的“证书颁发机构属性”对话框。在“设置”选项卡中，指定适当的设置如 HRA 要求

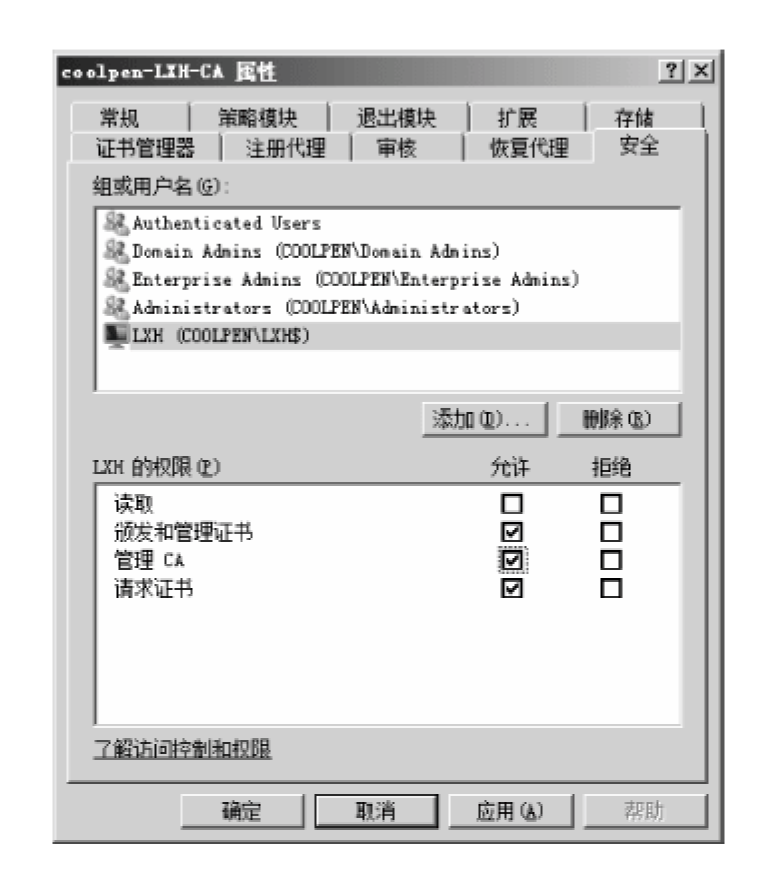


图 11-29 选择权限

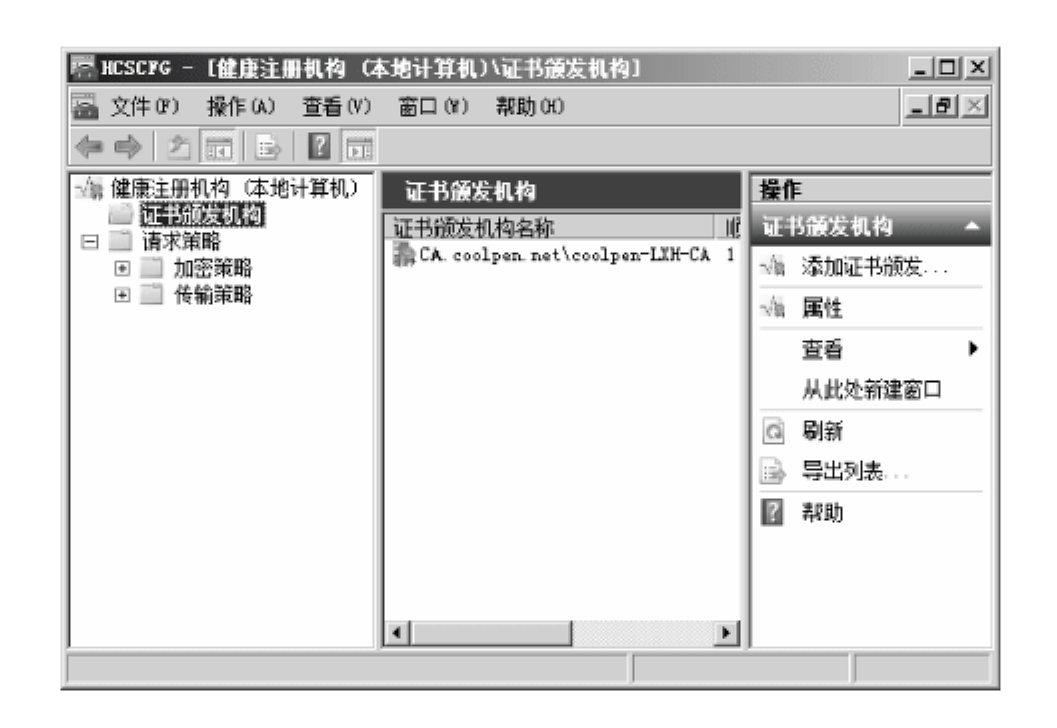



图 11-30　“健康注册机构(本地计算机)”窗口

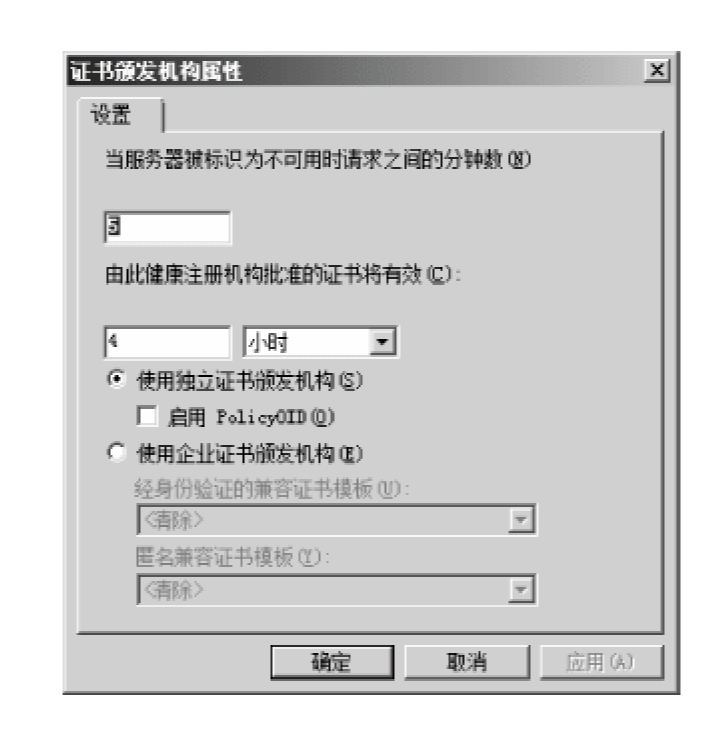


图 11-31　“证书颁发机构属性”对话框

的健康证书的有效时间,以及 HRA 是否使用独立或企业 CA。

(3) 单击“确定”按钮,保存设置即可。

4. 作为 RADIUS 代理在 HRA 上配置 NPS 服务

如果 NAP 健康策略服务器与 HRA 计算机位于不同的服务器上,则必须在 HRA 计算机上配置 NPS 服务作为 RADIUS 代理。允许 HRA 计算机作为 RADIUS 客户端,将基于 RADIUS 的请求发送到 NAP 健康策略服务器。

11.3.3　配置 NAP 健康策略服务器

为了配置 NAP 健康策略服务器,需要执行以下内容。

① 添加网络策略和访问服务角色。

② 安装 SHV。

③ 配置 RADIUS 服务器设置。

④ 为 IPSec 强制配置健康要求策略。

1. 配置 RADIUS 服务器设置

每个 NAP 健康策略服务器都是一个 RADIUS 服务,可能需要进行以下 RADIUS 服务器的设置。

① RADIUS 通信的 UDP 端口:通常只有在 NAP 健康策略服务也作为 RADIUS 服务器使用,并且其他 RADIUS 客户端使用与 RFC 定义的不同的端口时,才需要该步骤。NAP 健康策略服务器所使用的默认端口与 HRA 使用的端口相同。

② RADIUS 日志:用户可以配置 NPS 服务来记录入站请求和记账信息在本地文件中或 SQL 数据库服务器中。

注意:*必须使用 HRA 配置每个 NAP 健康策略服务器作为 RADIUS 客户端。*

(1) 在“网络策略服务器”管理单元中,展开“RADIUS 客户端和服务器”,右击“RADIUS 客户端”并在快捷菜单中选择“新建 RADIUS 客户端”选项,显示如图 11-32 所示的“新建 RADIUS 客户端”对话框。

(2) 在“友好名称”文本框中,输入 HRA 计算机的名称。在“地址(IP 或 DNS)”文本框中,输入 HRA 计算机的 IPv4 地址、IPv6 地址或 DNS 域名称。如果输入 DNS 域名称,需要单击“验证”按钮来解析名称为正确的 IP 地址。

（3）在“共享机密”区域，在“共享机密”和“确认共享机密”文本框中，输入 NPS 服务器和 HRA 计算机联合的共享机密，或者单击“生成”按钮使 NPS 服务生成一个 RADIUS 共享机密。

（4）选中“RADIUS 客户端支持 NAP”复选框。

（5）单击“确定”按钮，确认并保存设置。为每个 HRA 重复以上步骤，发送健康评估请求到 NAP 健康策略服务器。

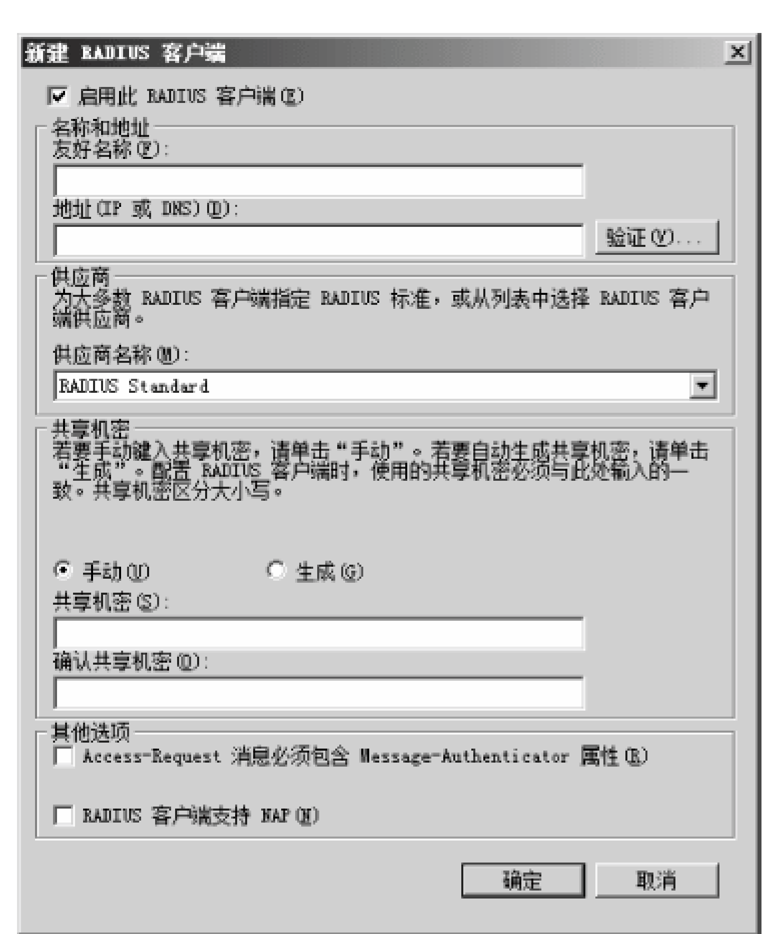


图 11-32 “新建 RADIUS 客户端”对话框

2. 创建 IPSec 强制策略

建议用户使用“配置 NAP 向导”创建相关策略，详细操作过程参照本书“网络访问保护概述”中的相关介绍。接下来，只是根据需要对网络策略进行配置。使用“配置 NAP 向导”创建的网络策略只包括“符合”和“不符合”两种情况，因此，如果当前网络中包含不支持 NAP 功能的客户端，还需要为其制定健康要求策略。

（1）在“网络策略服务器”管理单元中，展开“策略”选项，选择“网络策略”选项。如果在“选择与 NAP 一起使用的网络连接方法”中使用 IPSec 作为名称，那么不符合的 NAP 客户端的网络策略名称就是“IPSec 不符合”，如图 11-33 所示。默认情况下，向导创建的网络策略已经启用。



图 11-33 网络策略

（2）双击“IPSec 符合”策略，显示如图 11-34 所示的“IPSec 符合 属性”对话框，切换至“设置”选项卡，单击“NAP 强制”选项，确保已经选中“允许完全网络访问”单选按钮，即符合健康策略要求的计算机可以进行正常网络访问。

（3）双击“IPSec 不符合”策略，显示如图 11-35 所示的“IPSec 不符合 属性”对话框，切换至“设置”选项卡，单击“NAP 强制”选项，确保已经选中“允许受限访问”单选按钮，即不符合健康策略要求的客户端的网络访问将受到限制。



图 11-34　“IPSec 符合 属性”对话框

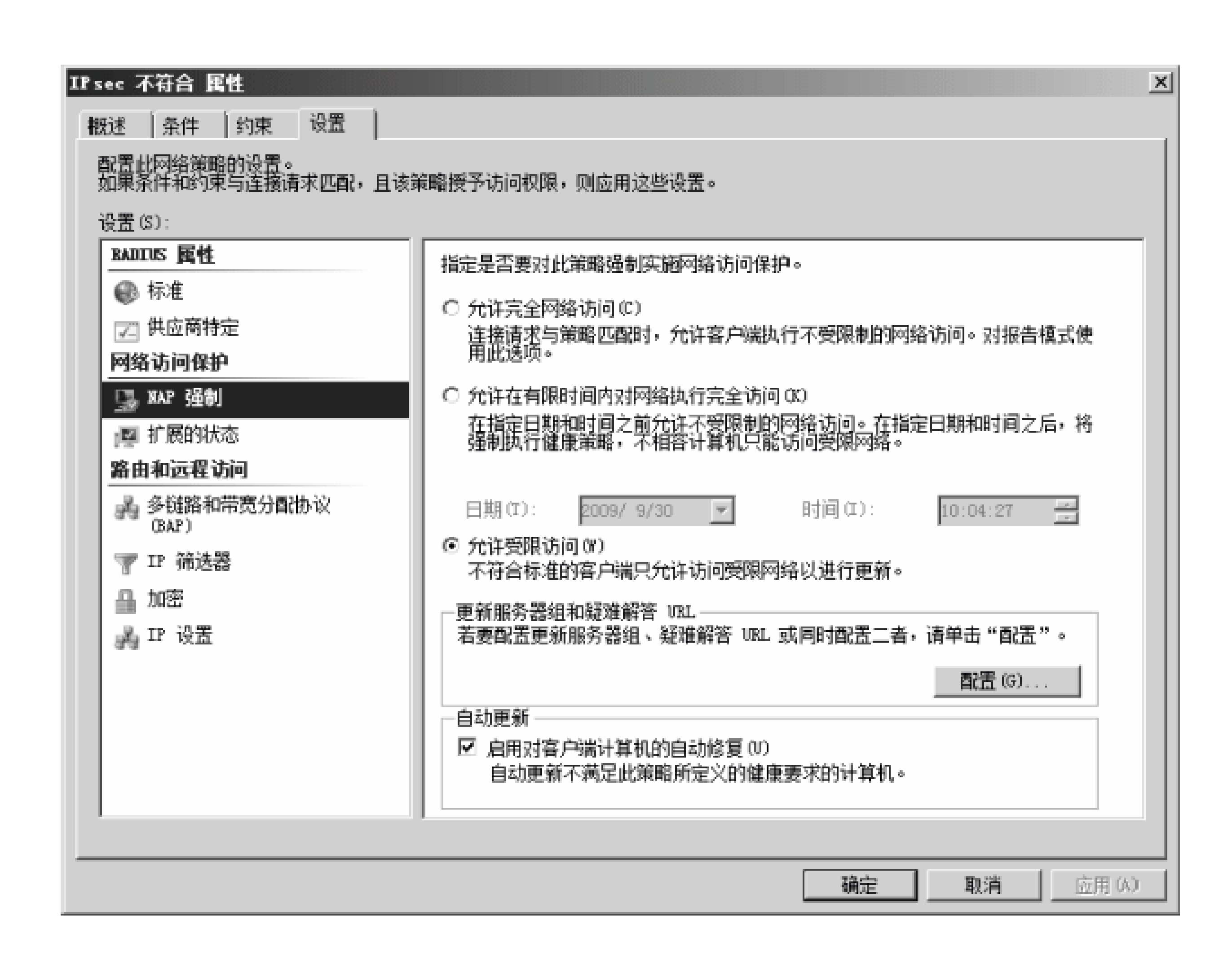


图 11-35　“IPSec 不符合 属性”对话框

(4) 在“更新服务器组和疑难解答 URL”区域，单击“配置”按钮，显示如图 11-36 所示的“更新服务器和疑难解答 URL”对话框，如果前期准备工作中已经部署了更新服务器组，则在此处选择希望允许其使用的更新服务器即可。在“疑难解答 URL”文本框中，输入更新服务器的 Web 页面的 URL。该 URL 当用户单击“网络访问保护”对话框中的“详细信息”时是活动的。

(5) 如果没有准备好 NAP 强制所需的更新服务器组，则可以在这里单击“新建组”按钮，显示如图 11-37 所示的“新建更新服务器组”对话框，在“组名”文本框中，输入更新服务器组的名称，例如 WSUS 等。单击“添加”按钮，即可开始向该组中添加更新服务器。更新服务器组中通常包括 DHCP 服务器、DNS 服务器、WSUS 服务器和防病毒服务器等。完成后，连续单击“确定”按钮保存设置即可。

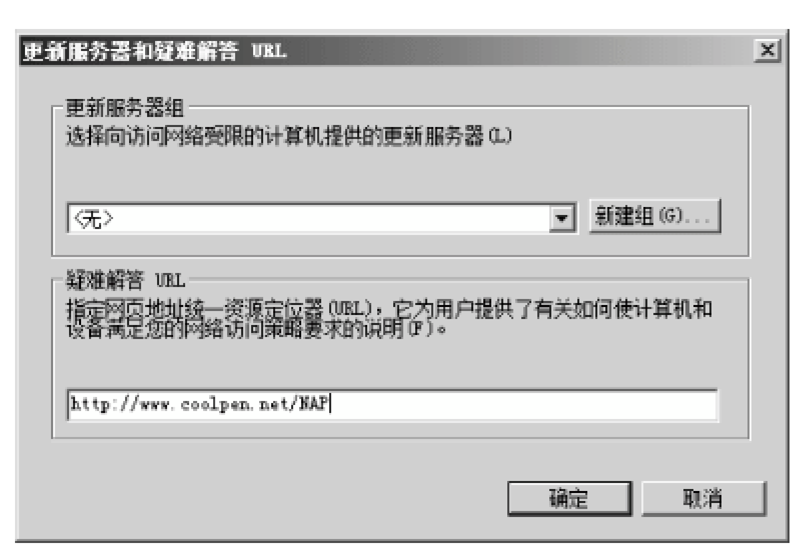


图 11-36 “更新服务器和疑难解答 URL”对话框

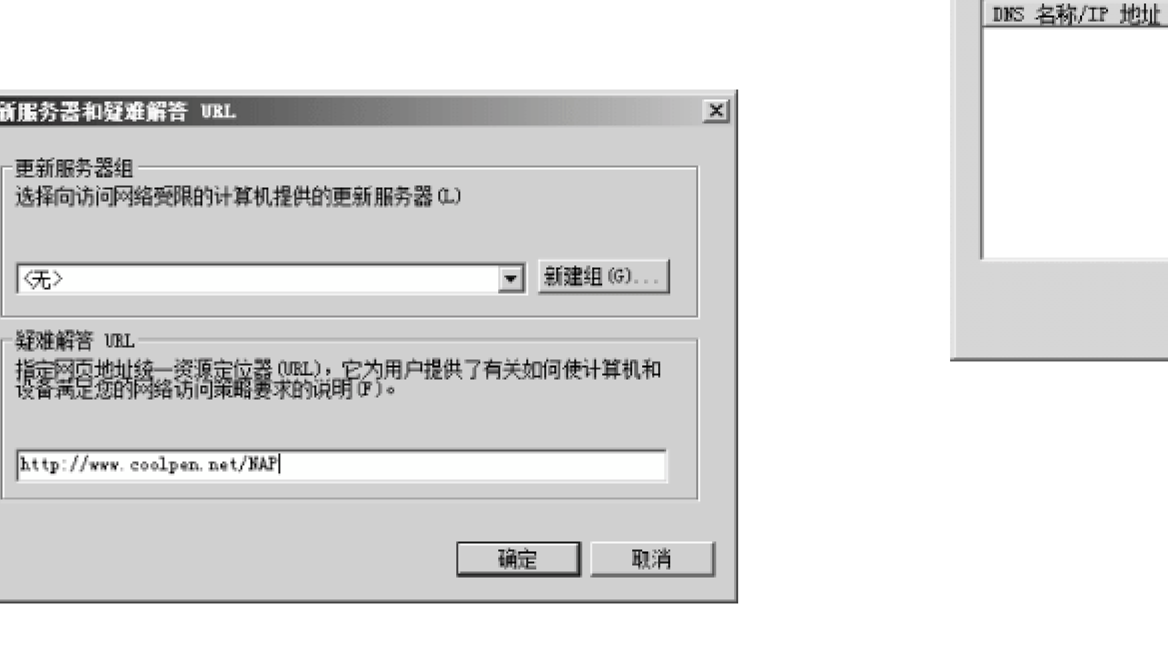


图 11-37 “新建更新服务器组”对话框

（6）为非 NAP 客户端创建网络策略。并非所有 Windows 操作系统都支持 NAP 客户端，因此用户应为此类计算机创建单独网络访问策略，建议允许其完全访问。在“网络策略服务器”窗口的“网络策略”列表中，创建非 NAP 客户端的 IPSec 强制策略。用户可以右击“网络策略”选择快捷菜单中的“新建”选项，启动“新建网络策略”向导来创建网络策略，也可以直接复制现有网络策略，然后对其进行相应配置，建议采用第二种方式。例如，右击“IPSec 不符合”策略，选择快捷菜单中的“重复策略”选项，即可创建新的网络策略。将复制后的策略命名为“IPSec 非 NAP 客户端”，并将其上移到最顶端，确保被优先处理，如图 11-38 所示。

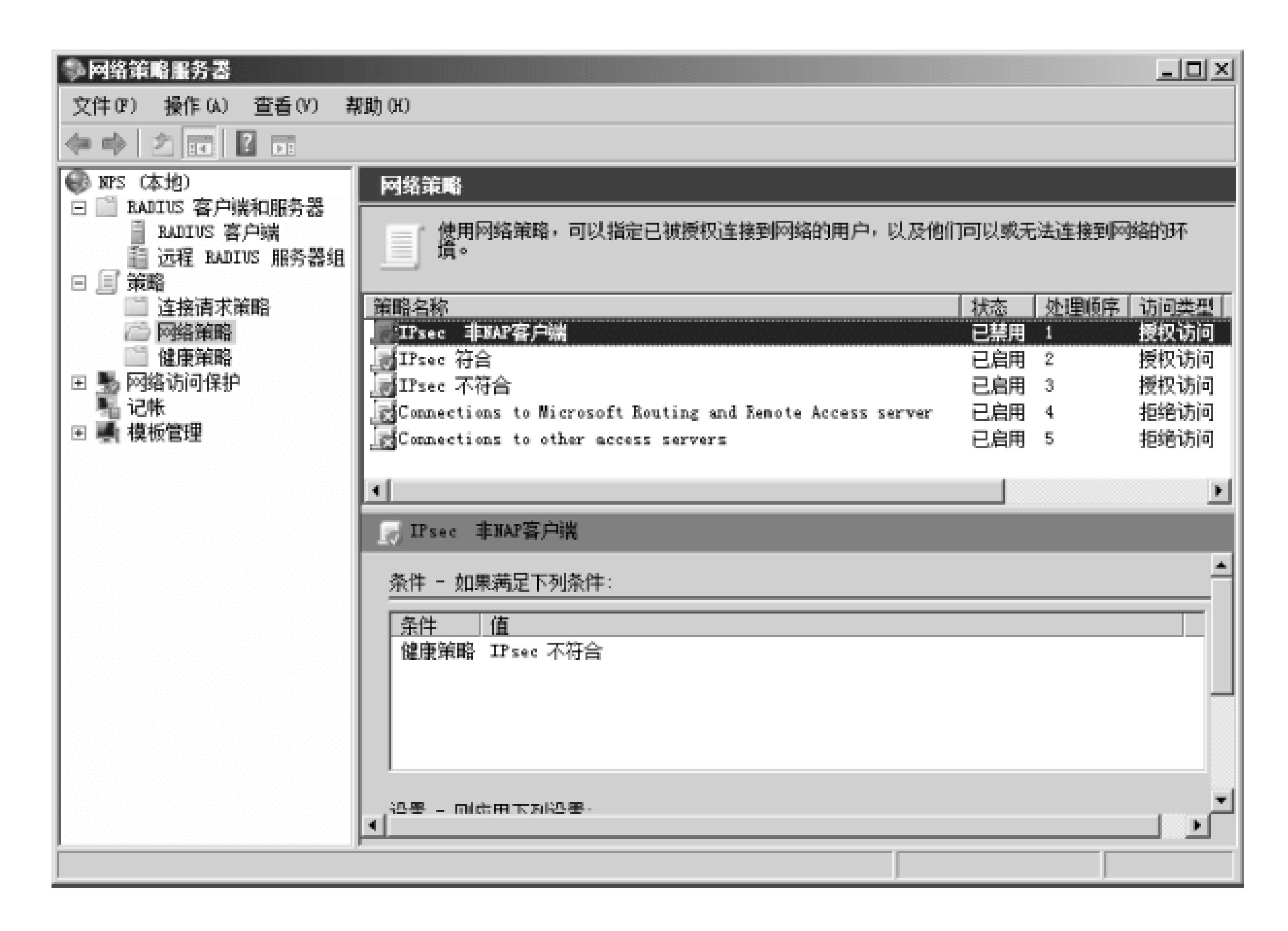


图 11-38 为非 NAP 客户端创建网络策略

（7）双击“IPSec 非 NAP 客户端”策略，显示“IPSec 非 NAP 客户端 属性”对话框，默认显示“概述”选项卡。复制后的新网络策略默认是禁用的，可以在这里选中“策略已启用”复选框将其启用，如图 11-39 所示。

（8）切换至如图 11-40 所示的“条件”选项卡，配置此网络策略的条件。由于该策略是由“IPSec 不符合”策略重复而来的，所以仍然保留着原有条件。在这里需要将其删除。

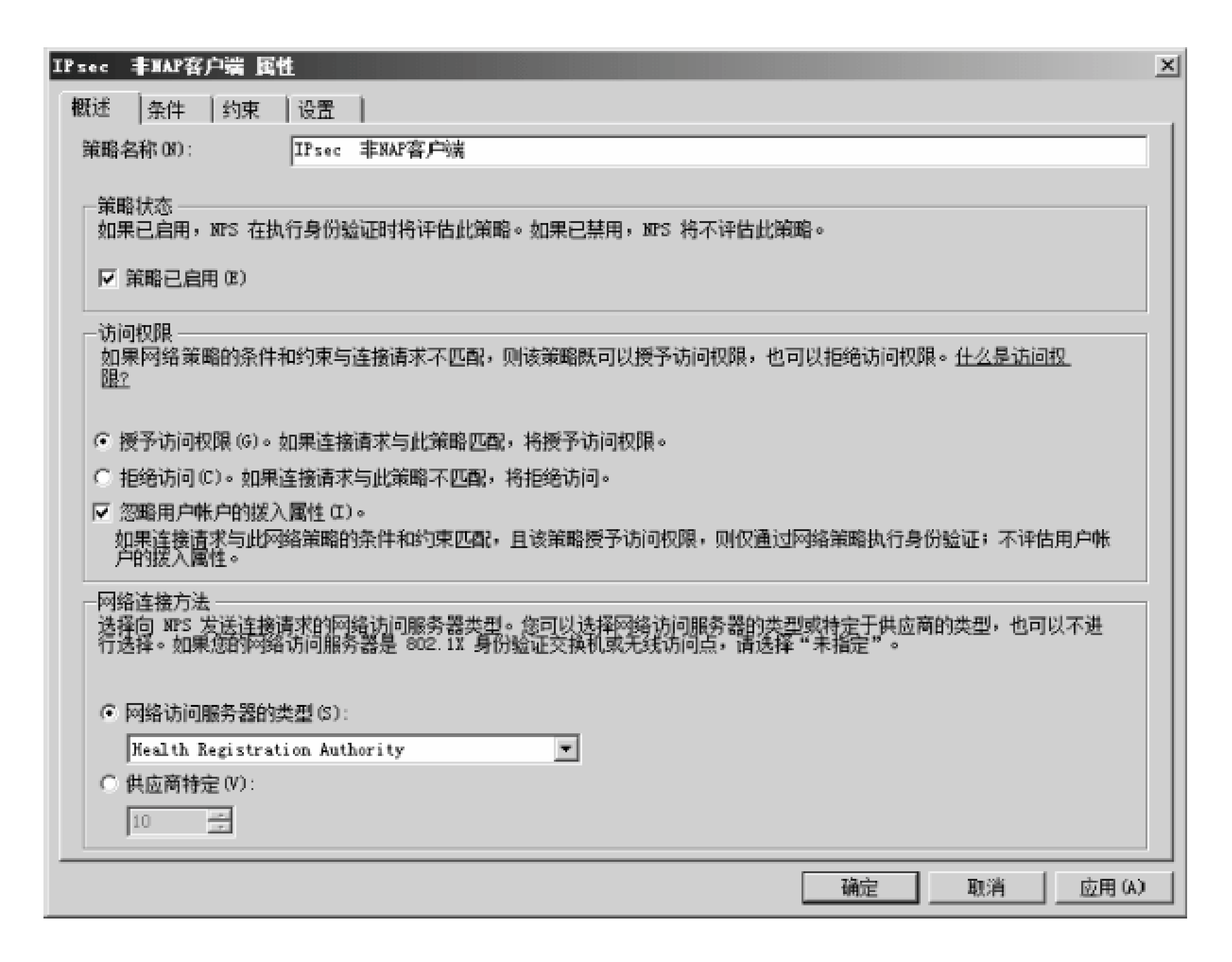


图 11-39 “概述”选项卡

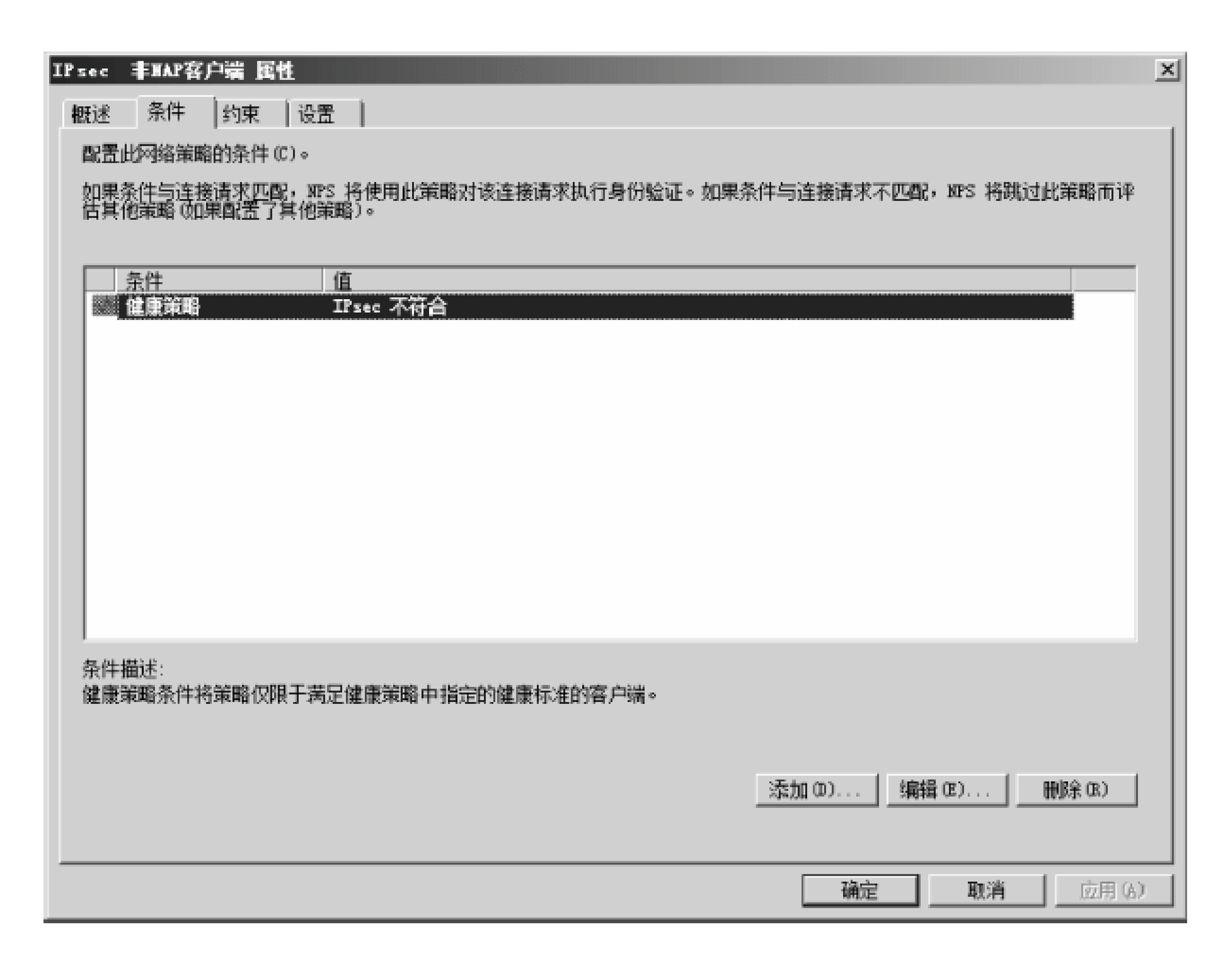


图 11-40 “条件”选项卡

（9）单击“添加”按钮，显示“选择条件”对话框，选中“支持 NAP 的计算机”，单击“添加”按钮，显示“支持 NAP 的计算机”对话框，选中“仅限不支持 NAP 的计算机”单选按钮，如图 11-41 所示。连续单击“确定”按钮，返回“IPSec 非 NAP 客户端 属性”对话框。

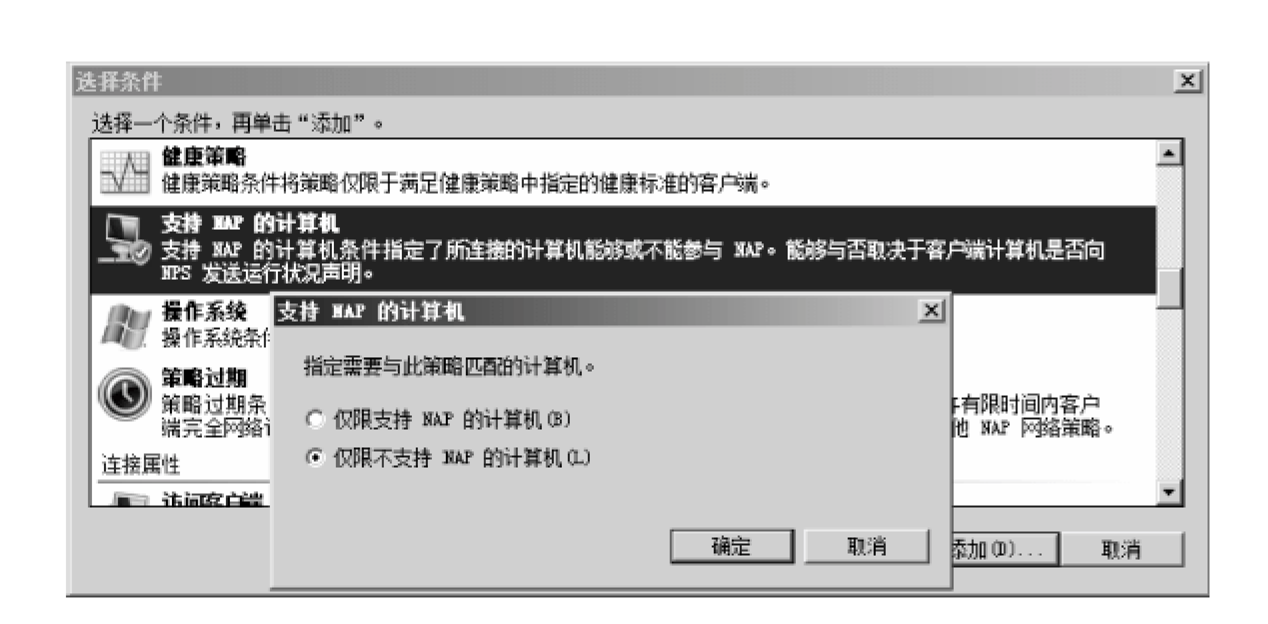


图 11-41 “选择条件”对话框

（10）切换至如图 11-42 所示的“设置”选项卡，选中“允许完全网络访问”单选按钮，即允许非 NAP 客户端正常访问网络。如果需要限制此类用户访问，则可以选择其他强制类型。



图 11-42 “设置”选项卡

（11）单击“确定”按钮，保存设置。

3. 配置 SHV

（1）在“网络策略服务器”管理单元中，依次展开“网络访问保护”→“系统健康验证器”选项，在右侧栏中，双击 SHV，然后配置每个 SHV 的系统健康要求。例如，双击“Windows 安全健康验证程序”，显示如图 11-43 所示的“Windows 安全健康验证程序 属性”对话框。

（2）单击“配置”按钮，显示如图 11-44 所示的“Windows 安全健康验证程序”对话框，根据需要配置基于 Windows Vista 和 Windows XP 的系统健康要求即可。



图 11-43 “Windows 安全健康验证程序 属性”对话框



图 11-44 “Windows 安全健康验证程序”对话框

提示：确保健康策略配置了正确的SHV，以及影响健康要求的条件，还可以对健康策略中的每个条件进行选择。

（3）配置完成后，单击“确定”按钮，保存设置即可。

11.3.4 使用组策略配置NAP客户端

默认情况下，Windows系统中的NAP客户端并未启用，用户可以根据需要启用相关的强制客户端类型。如果是独立计算机，则可以在客户端计算机上分别配置；在域网络中，建议使用组策略统一部署NAP客户端，主要包括以下任务。

① 配置NAP客户端设置。

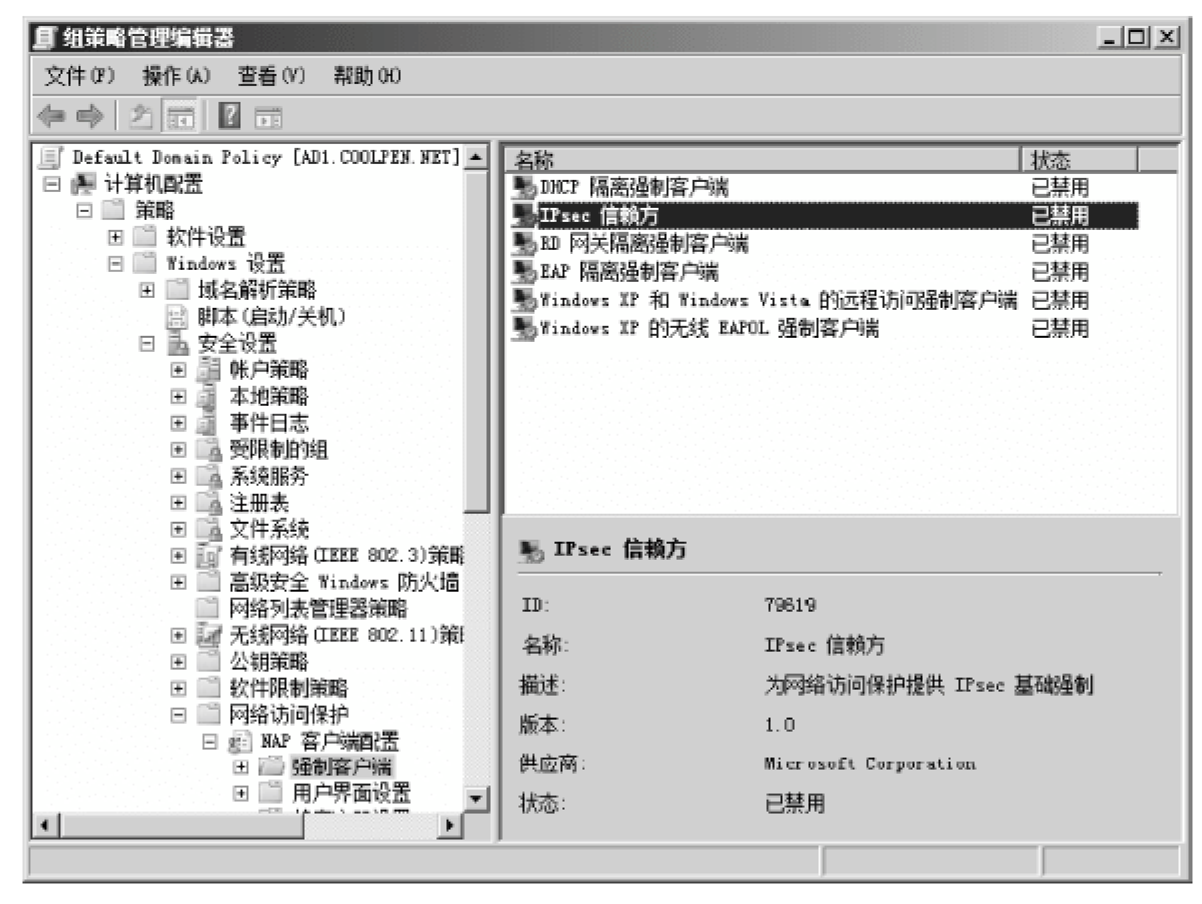
② 启用Windows安全中心。

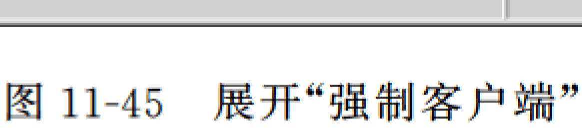
③ 配置网络访问保护代理服务的自动启用。

1. NAP客户端的设置

（1）在“组策略管理器”管理单元中，依次展开“林”→“域”选项。在“链接的组策略对象”面板中，右击组策略对象（默认对象是Default Domain Policy），在快捷菜单中选择“编辑”选项，打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows设置”→“安全设置”→“网络访问保护”→“NAP客户端配置”→“强制客户端”选项，如图11-45所示。

（2）在右侧主窗口中，双击“IPSec信赖方”强制客户端，显示如图11-46所示的“IPSec信赖方 个属性”对话框，选中“启用此强制客户端”复选框。




图11-45 展开“强制客户端”

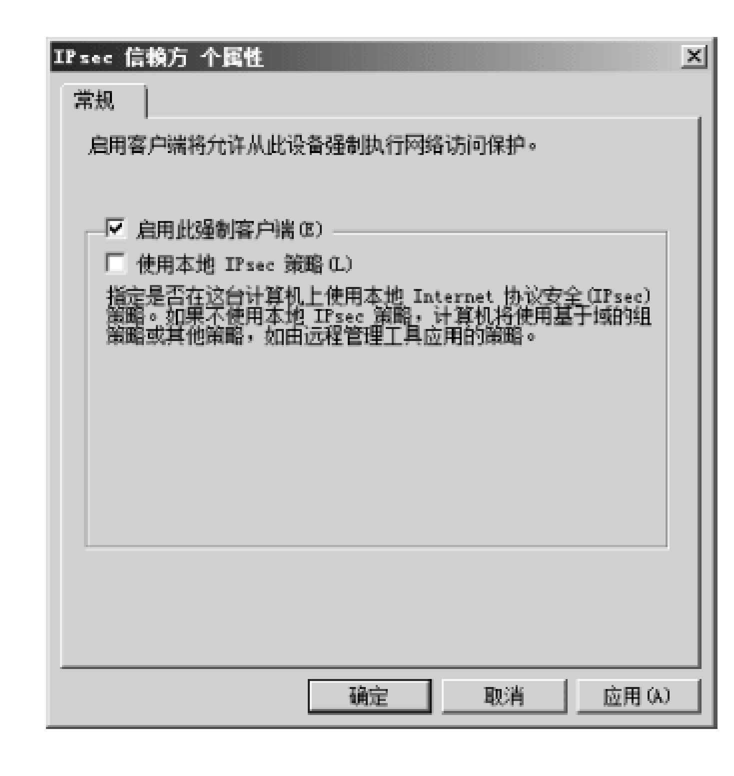


图11-46 “IPSec信赖方 个属性”对话框

（3）单击“确定”按钮，保存设置。

（4）如果使用受信任的服务器组作为NAP客户端查找HRA的方法，则可在控制台中展开“健康注册设置”，如图11-47所示。

（5）添加受信任服务器组。右击“受信任服务器组”，在快捷菜单中选择“新建”选项，显示如图11-48所示的“组名”对话框。在“组名”文本框中输入组名称。

（6）单击“下一步”按钮，显示如图11-49所示的“添加服务器”对话框。根据需要在“添加您希望客户端信任的健康注册机构的URL”文本框中，输入为应用组策略对象的NAP客户端所使用的HRA添加URL。

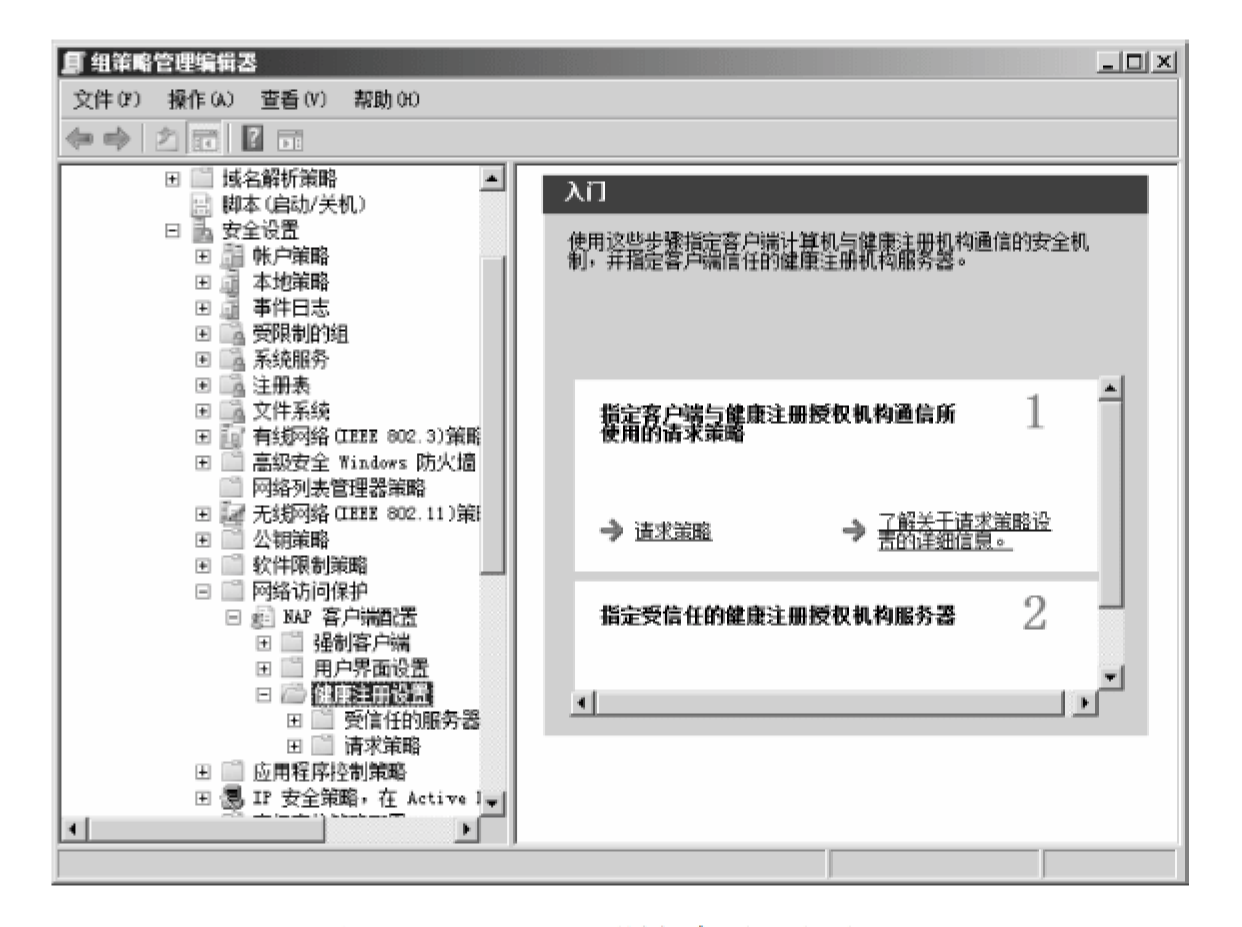


图 11-47 展开“健康注册设置”







图 11-48 “组名”对话框

图 11-49 “添加服务器”对话框

① 为使用 SSL 的 HTTP 认证健康证书，URL 必须采用以下形式：

https://HRA_FQDN/domainhra/hcsrvext.dll

其中 HRA_FQDN 为 HRA 计算机的 FQDN。

② 为认证使用 HTTP 的健康证书，URL 必须采用以下形式：

http://HRA_FQDN/domainhra/hcsrvext.dll

③ 为认证使用通过 SSL 的 HTTP 的匿名健康证书，URL 必须采用以下形式：

https://HRA_FQDN/nondomainhra/hcsrvext.dll

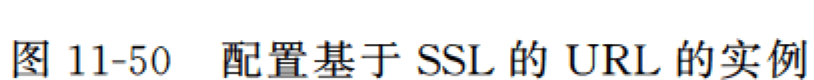
④ 为认证使用 HTTP 的匿名健康证书，URL 必须采用以下形式：

http://HRA_FQDN/nondomainhra/hcsrvext.dll

如果想要所有 URL 都基于 SSL，则需要选中“要求对此组中的所有服务器进行服务器验证(https:)”复选框。如果任意一个 URL 不是基于 SSL 的，则取消选中“要求对此组中的所有服务器进行服务器验证(https:)”复选框，图 11-50 所示为当所有 URL 都是基于 SSL 的实例。验证列表中的所有 URL 是否按照正确的顺序，如果需调整，则可以单击“上移”、“下移”按钮来实现。

（7）单击“下一步”按钮，显示如图 11-51 所示的“正在完成新建受信任的服务器组向导”对话框。




图 11-50　配置基于 SSL 的 URL 的实例

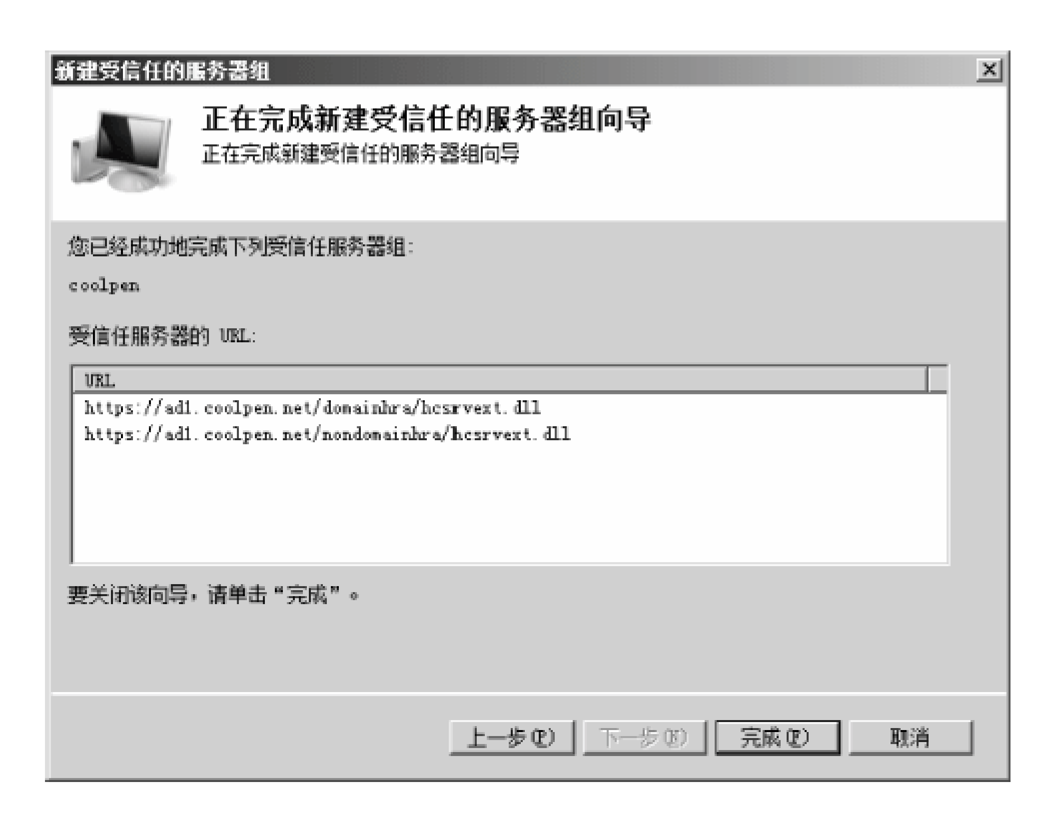


图 11-51　“正在完成新建受信任的服务器组向导”对话框

（8）单击“完成”按钮，完成添加受信任服务器组的操作。

2．启用 Windows 安全中心

（1）在“组策略管理”管理单元中，依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“安全中心”选项，如图 11-52 所示。

（2）双击“启用安全中心(仅限域 PC)”，显示如图 11-53 所示的“启用安全中心(仅限域 PC)属性”对话框，选中“已启用”单选按钮，用户还可以根据需要在“注释”选项卡中输入相关描述信息。



图 11-52　“安全中心”窗口

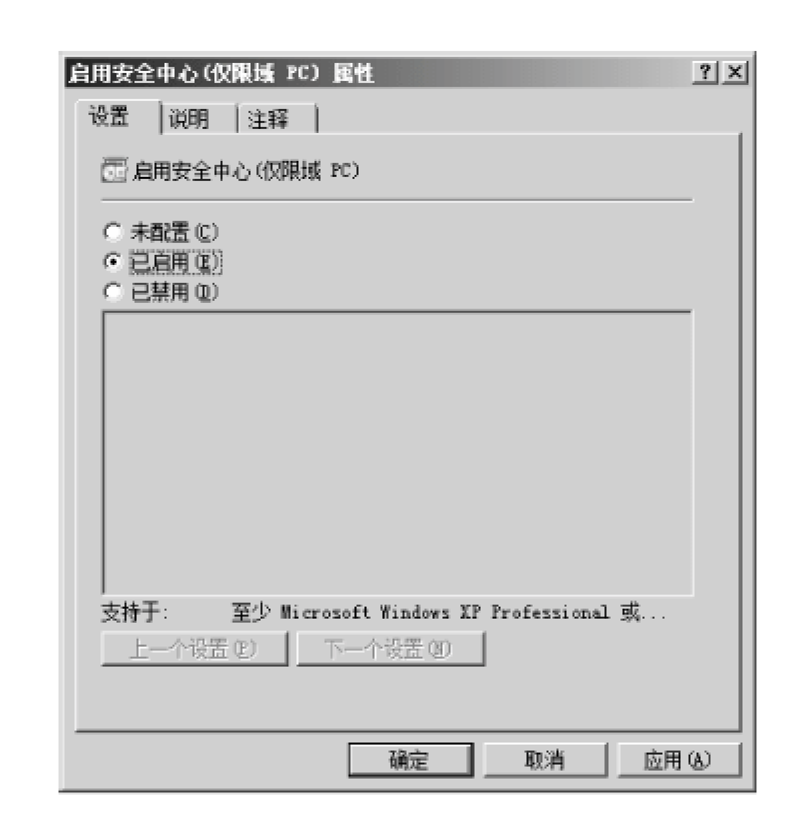


图 11-53　“启用安全中心(仅限域 PC)属性”对话框

（3）单击“确定”按钮，保存设置即可。

3．配置网络访问保护代理服务的自动启用

（1）在“组策略管理”管理单元中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“系统服务”选项。在详细面板中，双击 Network Access Protection Agent，显

示如图 11-54 所示的“Network Access Protection Agent 属性”对话框。选中“定义这个策略设置”复选框,并选中“自动”单选按钮。

(2) 单击“编辑安全设置”按钮,显示如图 11-55 所示的“安全设置 Network Access Protection Agent”对话框,确保客户端计算机账户对该服务拥有足够的控制权限。



图 11-54 “Network Access Protection Agent 属性”对话框

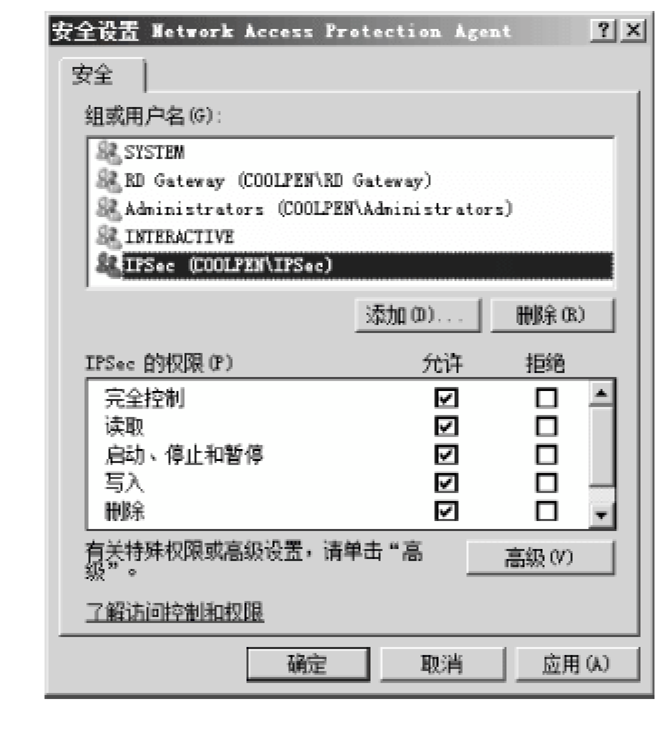


图 11-55 “安全设置 Network Access Protection Agent”对话框

(3) 连续单击“确定”按钮,保存设置。

提示:当使用组策略设置 NAP 客户端时,为了使用 DNS SRV 记录来配置 NAP 客户端发现 HRA,需要进行以下操作。

① 从 NAP 客户端组策略设置中删除所有已有受信任服务器组的配置。如果这些设置存在,NAP 客户端将不会使用 DNS SRV 记录来尝试发现 HRA。

② 在 NAP 客户端计算机上,创建和设置 HKLM\SOFTWARE\Policies\Microsoft\NetworkAccessProtection\ClientConfig\Enroll\HcsGroups\EnableDiscovery 的值为 1。

11.3.5 配置和应用 IPSec 策略

在验证了 NAP 客户端收到短期的健康证书和更新服务器收到长期的健康证书后,即可开始配置和应用 IPSec 策略到边界和安全网络中的计算机上。这需要执行以下步骤。

① 为边界网络配置和应用 IPSec 策略设置。

② 测试清空文本和与边界网络计算机的受保护的通信。

③ 为安全网络中的部分计算机配置和应用 IPSec 策略设置。

④ 测试清空文本和与安全网络计算机的受保护的通信。

⑤ 为延期强制模式的不符合的 NAP 客户端配置网络策略。

⑥ 为安全网络中所有的计算机配置和应用 IPSec 策略。

⑦ 为强制模式下的不符合的 NAP 客户端配置网络策略。

1. 为边界网络配置和应用 IPSec 策略设置

在这里需要创建包含 IPSec 策略设置的 GPO,请求为边界网络计算机的入站和出站通信进行 IPSec 保护。

(1) 在 Windows Server 2008 域控制器上,打开指定 GPO 的“组策略管理编辑器”窗

口，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙-LDAP”选项，如图 11-56 所示。

（2）右击“高级安全 Windows 防火墙-LDAP”，在快捷菜单中选择“属性”选项，显示如图 11-57 所示的“高级安全 Windows 防火墙-LDAP 属性”对话框。打开“域配置文件”选项卡，在“防火墙状态”下拉列表框中选择“启用(推荐)”选项，在“入站连接”下拉列表框中选择“阻止(默认值)”选项，在“出站连接”下拉列表框中选择“允许(默认值)”选项。



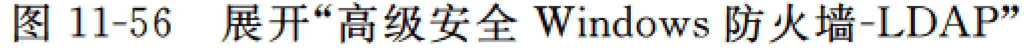

图 11-56　展开“高级安全 Windows 防火墙-LDAP”



图 11-57　“高级安全 Windows 防火墙-LDAP 属性”对话框

注意：“专用配置文件”和“公用配置文件”选项卡中的设置，与“域配置文件”相同，此处不再赘述。

（3）单击“确定”按钮，保存配置。

（4）在“高级安全 Windows 防火墙-LDAP”中，右击“连接安全规则”并在快捷菜单中选择“新规则”选项。显示“规则类型”对话框，选中“隔离”单选按钮。单击“下一步”按钮，显示如图 11-58 所示的“要求”对话框，选中“入站和出站连接请求身份验证”单选按钮。



图 11-58　“要求”对话框

(5) 单击“下一步”按钮,显示如图 11-59 所示的“身份验证方法”对话框。选中“计算机证书”单选按钮,然后单击“浏览”按钮,查看并选择所使用的证书,并选中“只接受健康证书”复选框。

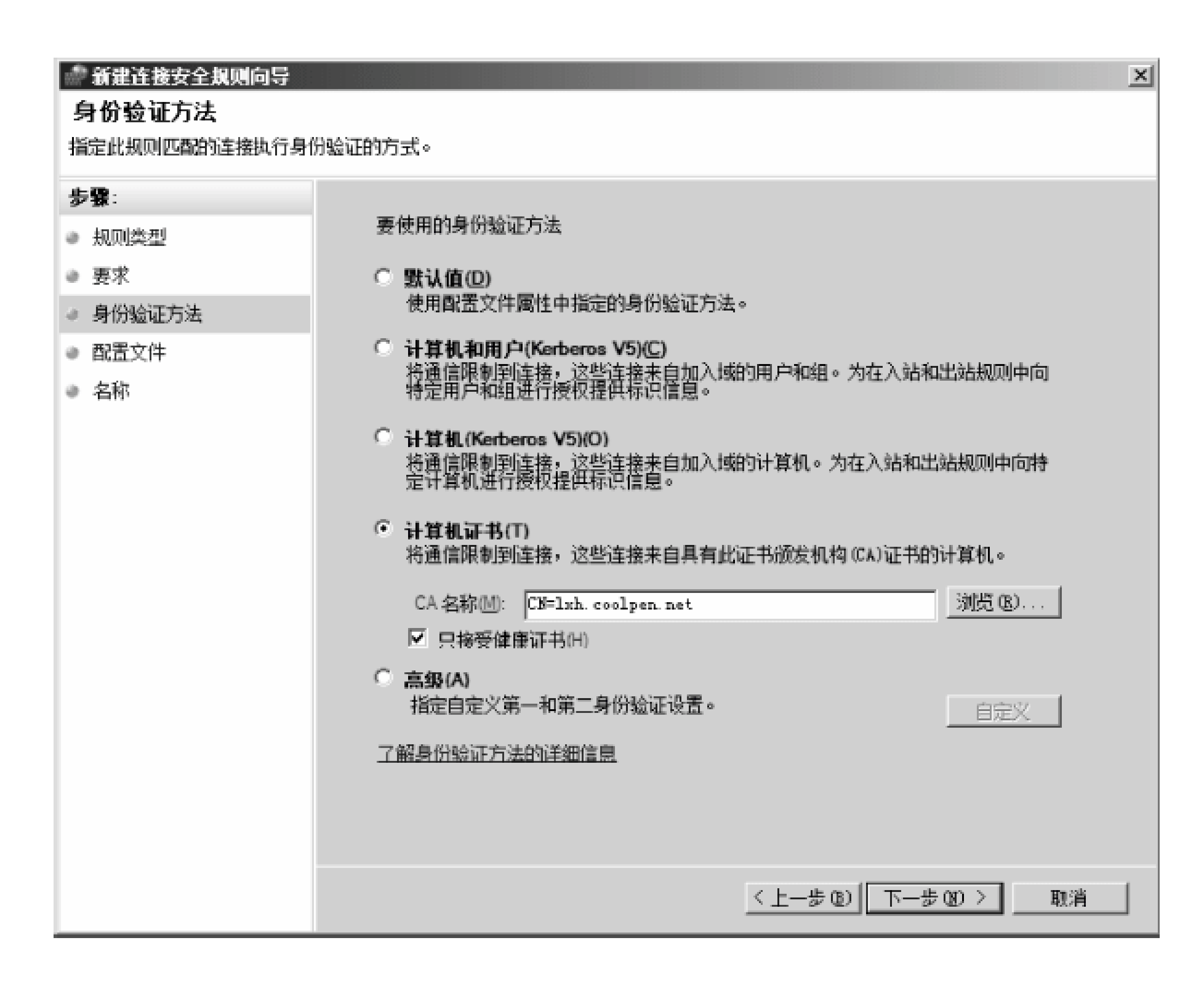


图 11-59 “身份验证方法”对话框

(6) 单击“下一步”按钮,显示如图 11-60 所示的“配置文件”对话框。选中“域”、“专用”和“公用”复选框。



图 11-60 “配置文件”对话框

(7) 单击“下一步”按钮,显示如图 11-61 所示的“名称”对话框。在“名称”文本框中,输入该规则的名称。在“描述”文本框中,输入该规则的描述信息。

(8) 单击“完成”按钮,完成新规则的配置。在创建完边界网络 GPO 后,需要将其应用于边界网络 OU 或安全组。

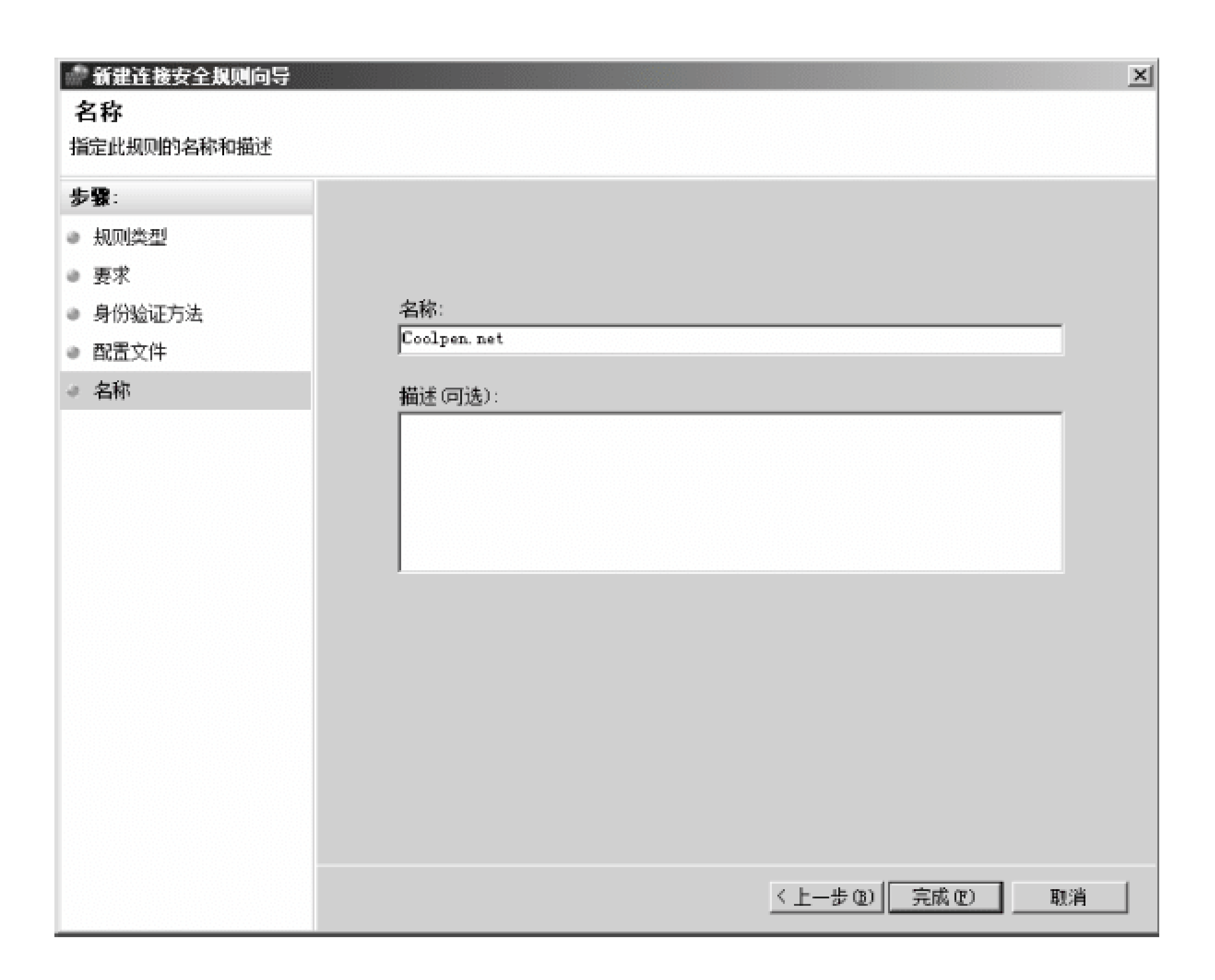


图 11-61 “名称”对话框

2. 测试与边界网络计算机的通信

在应用边界网络 GPO 到边界网络安全组或 OU 后,需要完成以下工作。

(1) 确保边界网络中的更新服务器能够收到边界网络 GPO 设置,并且拥有为入站和出站通信请求 IPSec 保护的连接安全规则。

(2) 如果更新服务器可以收到边界网络 GPO 的设置,确保更新服务器可以建立与 NAP 客户端和非域成员计算机的通信,并且 NAP 客户端和非域成员计算机可以建立与更新服务器的通信。

在该阶段的 NAP 客户端、非域成员计算机和更新服务器之间的通信应该清除文本。更新服务器上的 IPSec 策略将会尝试越过 IPSec 保护,但是允许回退清除入站和出站通信尝试。

3. 为安全网络中部分计算机配置和应用 IPSec 策略设置

在应用安全网络 GPO 到所有域成员计算机之前,用户应该在部分域成员计算机上测试安全网络 GPO,并且记录通信动作,可以使用以下方式实现。

(1) 包含测试计算机的安全测试网络 OU。在这种情况下,用户可以直接应用安全网络 GPO 到安全测试网络 OU 上,而不会影响到其他计算机。

(2) 包含测试计算机的安全测试网络安全组。在该情况下,用户必须为安全测试网络安全组筛选 GPO 的作用域,应用安全网络 GPO 到安全网络 OU 上。因为作用域的筛选,安全网络 GPO 将只会应用于安全测试网络安全组的成员上。

这里创建包括 IPSec 策略设置的 GPO,为安全网络计算机的入站和出站通信尝试提供 IPSec 保护。

(1) 在安装了组策略管理器的 Windows Server 2008 计算机上,打开 MMC 管理控制台,依次选择“开始”→“添加/删除管理单元”选项,显示“添加或删除管理单元”对话框。在“可用的管理单元”列表中,选择“组策略管理编辑器”选项。

(2) 单击“添加”按钮,显示“选择组策略对象”对话框。单击“浏览”按钮,查看并选择所

要编辑的组策略,如图 11-62 所示。单击“创建新的组策略对象”按钮,输入安全网络的新的组策略对象的名称。

(3) 单击“确定”按钮,返回“选择组策略对象”对话框。单击“完成”按钮,返回“添加或删除管理单元”对话框。再次单击“确定”按钮,完成管理单元的添加。

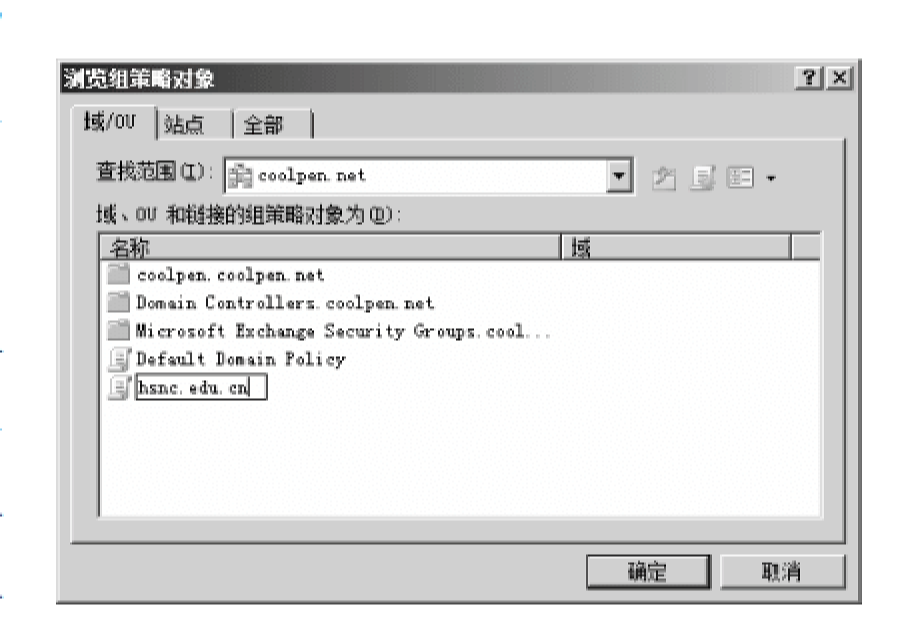


图 11-62 “浏览组策略对象”对话框

(4) 在控制台中,展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙-LDAP”选项。右击“高级安全 Windows 防火墙-LDAP”,在快捷菜单中选择“属性”选项。打开“高级安全 Windows 防火墙-LDAP”对话框,在“域配置文件”选项卡中的“防火墙状态”下拉列表框中选择“启用(推荐)”选项,在“入站连接”下拉列表框中选择“阻止(默认值)”选项,在“出站连接”下拉列表框中选择“允许(默认值)”选项。

(5) 切换到“专有配置文件”选项卡,在“防火墙状态”下拉列表框中选择“启用(推荐)”选项,在“入站连接”下拉列表框中选择“阻止(默认值)”选项,在“出站连接”下拉列表框中选择“允许(默认值)”选项。

(6) 切换到“公用配置文件”选项卡,在“防火墙状态”下拉列表框中选择“启用(推荐)”选项,在“入站连接”下拉列表框中选择“阻止(默认值)”选项,在“出站连接”下拉列表框中选择“允许(默认值)”选项。

(7) 单击“确定”按钮,保存设置。

(8) 在“高级安全 Windows 防火墙-LDAP”中,右击“连接安全规则”,在快捷菜单中选择“新规则”选项,打开“规则类型”对话框,选中“隔离”单选按钮。

(9) 单击“下一步”按钮,显示如图 11-63 所示的“要求”对话框,选中“入站连接要求身份验证,出站连接请求身份验证”单选按钮。

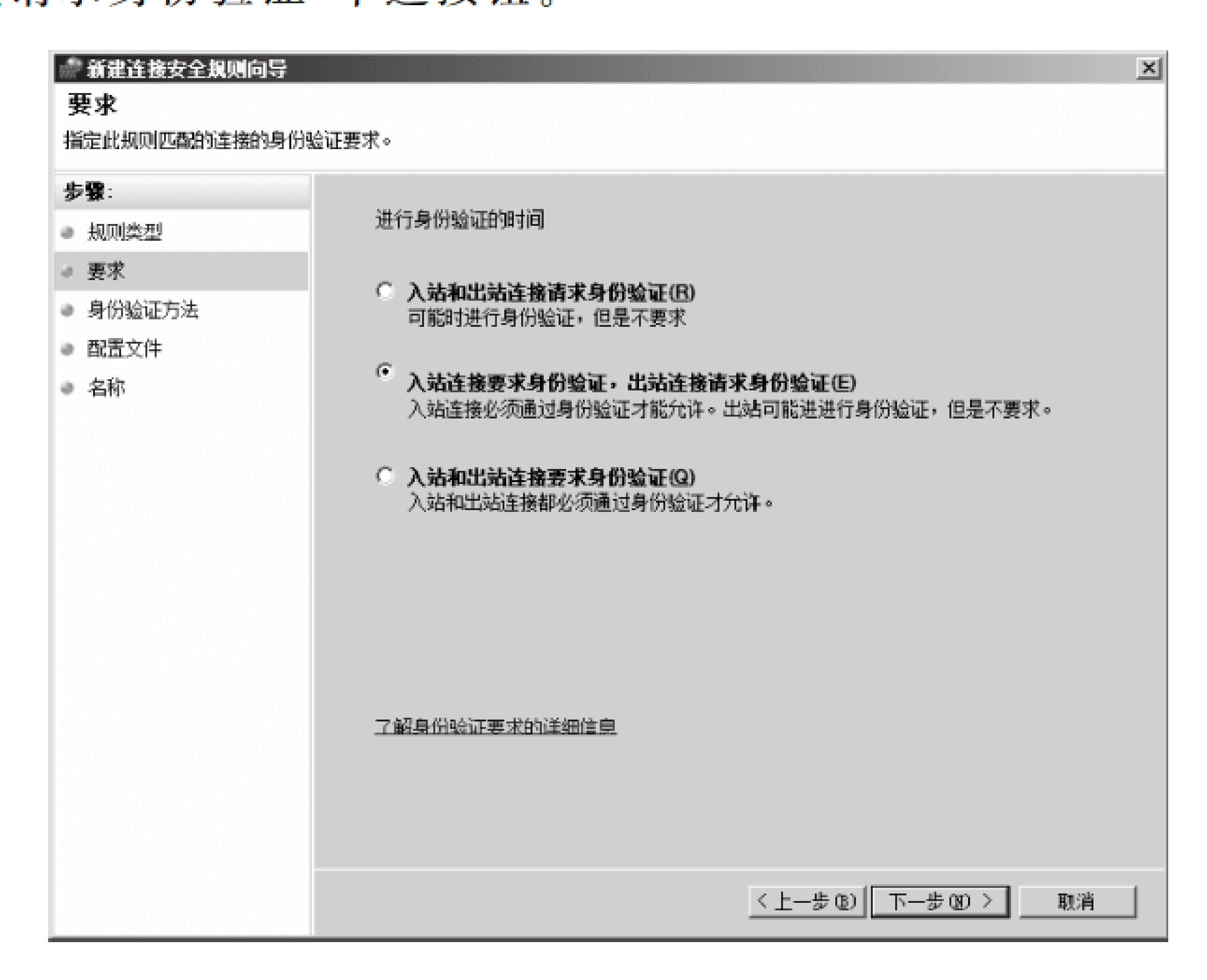


图 11-63 “要求”对话框

(10) 单击“下一步”按钮,打开“身份验证方法”对话框,选中“计算机证书”单选按钮,并选中“只接受健康证书”复选框,然后单击“浏览”按钮,查看并选择证书。

(11) 单击“下一步”按钮,打开“配置文件”对话框,同时选中“域”、“专用”和“公用”复选框。

(12) 单击“下一步”按钮,显示“名称”对话框。在“名称”文本框中,输入该规则的名称。在“描述”文本框中,输入该规则的描述信息。

对于运行 Windows XP SP3 的 NAP 客户端,必须使用“组策略编辑器”管理单元和活动目录中的“IP 安全策略”的“计算机配置\策略\Windows 设置\安全设置”来配置和启用同等的 IPSec 策略。另外,还必须设置 HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley\IKEFlags 的注册表值为 0x1c。

4. 测试清除文本和与安全网络部分计算机的受保护的通信

在配置完安全网络 GPO,并将其应用到安全测试网络 OU 或安全组后,还必须测试以下类型的通信。

(1) 确保安全网络中的计算机能够收到安全网络 GPO 设置,并且拥有为入站要求 IPSec 保护和出站请求 IPSec 保护的连接安全规则。例如,可以使用安全网络计算机上的“高级安全 Windows 防火墙”管理单元中的“监视器”节点。

(2) 如果安全网络的计算机可以收到安全网络 GPO 的设置,需确保以下通信动作。

① 阻止从非安全测试网络的计算机到安全测试网络计算机的通信。

② 保护从安全测试网络中的计算机到另一个安全测试网络计算机的通信。

③ 允许从安全测试网络计算机到非安全测试网络计算机的通信,但是不被保护。

该阶段的安全测试网络计算机到所有非安全测试网络的计算机通信应该被清除文本。安全测试网络计算机的 IPSec 策略将会尝试越过 IPSec 保护,但是会允许回退清除入站和出站通信尝试。

5. 为延期强制下的不符合的 NAP 客户端配置网络策略

在测试完边界和安全测试网络的通信后,为延期强制模式确定日期。在该时间段内,不符合的 NAP 客户端不会收到健康证书,不能建立与之符合的 NAP 客户端的通信。在延期强制模式下,不符合的 NAP 客户端仍会收到健康证书,但是用户会收到一条信息,指示计算机不能按照系统健康要求进行动作。

(1) 在“网络策略服务器”管理单元中,依次展开“策略”→“网络策略”选项。

(2) 在右侧栏中,双击 NAP 向导创建的不符合的 NAP 客户端的网络策略,打开“策略属性”对话框。切换到“设置”选项卡,然后选择“NAP 强制”选项,如图 11-64 所示。在右侧栏中,选中“允许在有限时间内对网络执行完全访问”单选按钮,指定 NAP 健康策略服务器上配置的强制模式的日期和时间。

(3) 单击“确定”按钮,保存设置即可。网络中每个 NAP 健康策略服务器,都需要执行这些操作。

6. 为安全网络中所有计算机配置 IPSec 策略设置

在测试和验证完安全测试网络中的入站和出站通信后,即可应用安全网络 GPO 到安全网络所有计算机上。为了应用安全网络 GPO 到包含所有域成员 NAP 客户端的安全网络 OU 或组,并且保证安全测试网络 OU 或组中的计算机得到适当的移植,具体可通过以下



图 11-64 “设置”选项卡

方法实现。

(1) 如果使用安全测试网络 OU 和包括所有域成员 NAP 客户端的安全网络 OU，则需要应用安全网络 GPO 到安全网络 OU，并且将安全测试网络 OU 中的计算机移植到安全网络 OU 中。

(2) 如果使用安全测试网络 OU 和包含所有域成员 NAP 客户端的安全网络安全组，则需应用安全网络 GPO 到安全网络 OU 中，并且确保安全测试网络 OU 中的计算机是安全网络 OU 中的成员。

(3) 如果使用安全测试网络安全组和包含所有域成员 NAP 客户端的安全网络 OU，则需应用安全网络 GPO 到安全网络 OU 中，并且确保安全测试网络安全组中的计算机是安全网络 OU 的成员。

(4) 如果使用安全测试网络安全组和包含所有域成员 NAP 客户端的安全网络安全组，则应更改安全网络 GPO 的作用域筛选，保证其应用于安全网络安全组中，并且确保安全测试网络安全组中的计算机是安全网络安全组的成员。

7. 为强制模式下的不符合的 NAP 客户端配置网络策略

在强制模式的日期中，配置 NAP 健康策略服务器的强制模式的具体操作步骤如下。

(1) 在“网络策略服务器”管理单元中，依次展开“策略”→“网络策略”选项。

(2) 在右侧栏中，双击不符合的 NAP 客户端的网络策略，打开“策略 属性”对话框。切换到“设置”选项卡，然后选择“NAP 强制”。并选中“允许在有限时间内对网络执行完全访问”单选按钮。

(3) 单击“确定”按钮，保存设置即可。

至此，IPSec 强制的配置已经完成，不符合的 NAP 客户端将不会收到健康证书，并且安全网络中的计算机对入站连接请求要求 IPSec 保护和健康证书。

11.4 配置 802.1x 强制

通过 802.1x 强制，可以确保未经许可的网络设备或移动客户端接入企业网络。配置 802.1x 强制包括配置活动目录、配置基于 PEAP 的身份验证方式、配置 802.1x 访问点、配置受限网络的更新服务器、配置 NAP 健康策略服务器和配置 NAP 客户端等内容。

11.4.1 配置基于 PEAP 的身份验证方式

如果没有为 802.1x 身份验证的无线或有线访问使用基于 PEAP 的身份验证方式，那么用户必须重新配置访问客户端和 NPS 服务器上的访问策略。在 Windows Server 2008 和 Windows Vista 中，支持以下有线身份验证的 EAP 身份验证方法：

① EAP-TLS

② PEAP-MS-CHAP v2

③ PEAP-TLS

EAP-TLS 和 PEAP-TLS 可以与 PKI 和计算机证书、用户证书和智能卡联合使用。使用 EAP-TLS，有线客户端为身份验证发送自己的计算机证书、用户证书或智能卡。

1. 身份验证方法的需求

有线身份验证方法的需求如下。

(1) EAP-TLS 需要在每台 RADIUS 服务器上安装计算机证书，在所有有线客户端上安装计算机证书、用户证书或智能卡。为了验证 RADIUS 服务器上的计算机证书，RADIUS 服务器计算机证书发布 CA 的根 CA 证书必须安装在所有有线客户端计算机上。为了验证有线客户端的计算机证书、用户证书或智能卡，有线客户端证书的发布 CA 的根 CA 证书必须安装在每台 RADIUS 服务器上。

(2) PEAP-MS-CHAP v2 需要在每台 RADIUS 服务器上安装计算机证书，并且为了验证 RADIUS 服务器上的计算机证书，RADIUS 服务器计算机证书发布 CA 的根 CA 证书必须安装在所有有线客户端计算机上。

在没有计算机证书、用户证书或智能卡的情况下，可以使用 PEAP-MS-CHAP v2。PEAP-MS-CHAP v2 是一种基于密码的身份验证方法，使用加密的 TLS 会话交换身份验证消息。加密 TLS 会话的使用使得恶意用户很难从捕获的身份验证消息中获取密码。因为 EAP-TLS 和 PEAP-TLS 不依赖于密码，所以它们比 PEAP-MS-CHAP v2 要安全得多。

2. 有线网络(IEEE 802.3)策略组策略扩展

为了 Windows 有线客户端计算机自动配置有线网络设置，Windows Server 2008 或 Windows Server 2003 活动目录域支持有线网络(IEEE 802.3)策略组策略扩展。该扩展允许将有线网络设置，作为基于域的组策略对象的计算机配置组策略的一部分进行配置。通过使用有线网络(IEEE 802.3)策略组策略扩展，可以在 Windows Server 2008 或 Windows Vista 有线客户端上，指定 EAP 身份验证方法和其他设置。

(1) 打开相应策略的“组策略对象编辑器”窗口，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“有线网络(IEEE 802.3)策略”选项。默认情况下，没有任何有线网络(IEEE 802.3)策略，根据需要可以创建一个新的策略，右击“有线网络(IEEE 802.3)

策略”，在快捷菜单中选择“创建一个新的 Windows Vista 策略”选项，显示如图 11-65 所示的“新 Vista 有线网络策略 Properties”对话框。

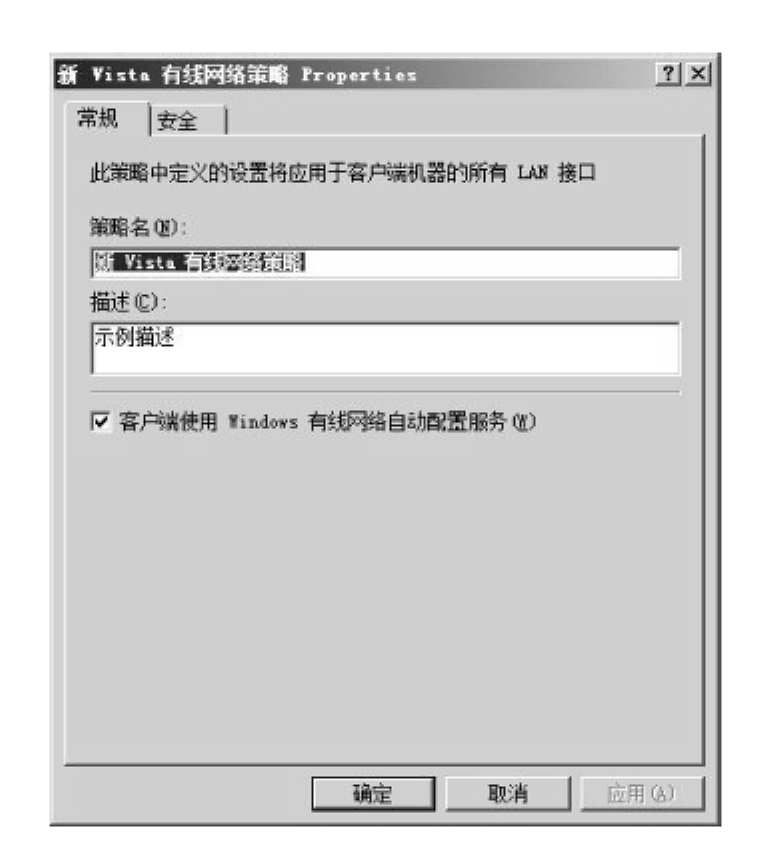


图 11-65 “新 Vista 有线网络策略 Properties”对话框

(2) 在“常规”选项卡中，配置策略的名称和描述，指定是否启用有线自动配置服务。切换到如图 11-66 所示的“安全”选项卡中，选中“为网络访问启用 IEEE 802.1x 身份验证”复选框，启用 802.1x 身份验证。根据需要在“选择网络身份验证方法”下拉列表框中，选择所需的身份验证方法。

(3) 单击“高级”按钮，显示如图 11-67 所示的“高级安全设置”对话框，根据需要，可以配置 802.1x 和单一登录的高级设置。具体各选项含义如下。

① 最大 Eapol 启动消息数：当发出的最初 EAPOL-Start 消息没有回应时，连续发送的 EAPOL-Start 消息的数目。

② 保持时间：当最初 EAPOL-Start 消息没有回应时，重发的 EAPOL-Start 消息之间的间隔时间。

③ 启动时间：这段时间内认证客户端将不执行任何 802.1x 身份验证活动。

④ 验证时间：认证客户端在重发 802.1x 请求之前等待的时间。

(4) 配置完成后，单击“确定”按钮，保存设置。

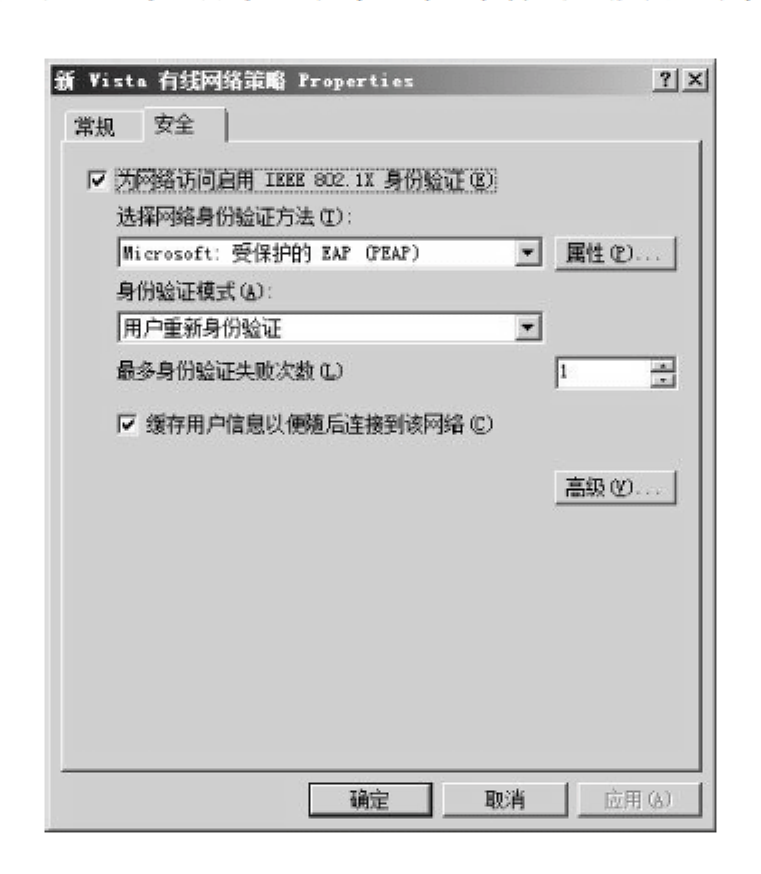


图 11-66 “安全”选项卡



图 11-67 “高级安全设置”对话框

11.4.2 配置 802.1x 访问点

为了在 802.1x 强制中使用 ACL，需要完成以下工作。

(1) 使用 ACL 配置 802.1x 访问点，限制不符合的 NAP 客户端的访问。ACL 必须包含符合内网更新服务器通信的数据包筛选列表。

(2) 确定通过 802.1x 访问点的 RADIUS 属性识别受限网络访问的 ACL，某些 802.1x 访问使用标准的 RADIUS 属性筛选 ID。

为了在 802.1x 强制中使用 VLAN，需要完成以下工作。

（1）如果使用 VLAN 访问内网，那么 VLAN 就变为符合的 NAP 客户端的 VLAN。在这种情况下，只需要为不符合的 NAP 客户端，创建一个新的 VLAN 即可。

（2）确定通过 802.1x 访问点的 RADIUS 属性指出受限网络 VLAN，某些 802.1x 访问点使用如下 RADIUS 或指定供应商属性：Tunnel-Medium-Type、Tunnel-Pvt-Group-ID、Tunnel-Type 和 Tunnel-Tag。

11.4.3　配置 NAP 健康策略服务器

802.1x 强制的 NAP 健康策略服务器，与 802.1x 身份验证所使用的基于 NPS 的 RADIUS 服务器相同。关于配置 NAP 健康策略服务器，必须按照以下步骤修改现有 NPS 服务器的配置。

① 安装 SHV。

② 配置 RADIUS 服务器设置。

③ 为 802.1x 强制配置健康要求策略。

1. 配置 RADIUS 服务器设置

由于 NAP 健康策略服务器已经配置了 802.1x 身份验证，所以不需要对 RADIUS 服务器的通常配置进行更改，如 RADIUS 客户端或 UDP 端口。但因为 802.1x 强制配置开始时会使用报告模式，不符合的 NAP 客户端拥有不受限访问，所以可能想要在启用强制模式前使 NAP 健康策略服务器记录入站请求以便于分析。

2. 为无线或有线连接的 802.1x 强制创建策略

（1）登录 NPS 服务器，在"网络策略服务器"窗口中启动"配置 NAP"向导。在如图 11-68 所示的"选择与 NAP 一起使用的网络连接方法"对话框中，在"网络连接方法"下拉列表框中，选择"IEEE 802.1x(无线)"或者"IEEE 802.1x(有线)"选项，然后在"策略名称"文本框中，输入策略名称。

（2）在如图 11-69 所示的"配置身份验证方法"对话框中，为 PEAP 身份验证选择 NPS 所使用的计算机证书，然后根据需要选中"安全密码(PEAP-MS-CHAP v2)"或者"智能卡或其他证书(EAP-TLS)"复选框即可。

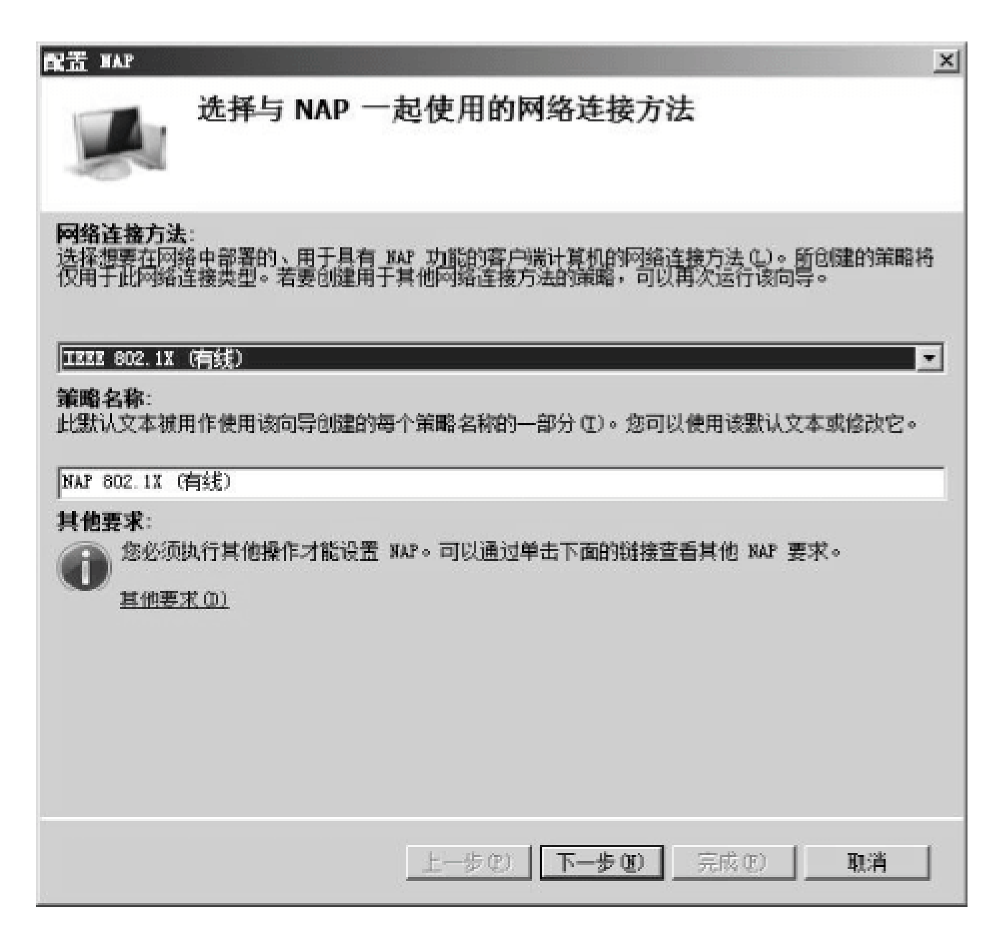


图 11-68　"选择与 NAP 一起使用的网络连接方法"对话框

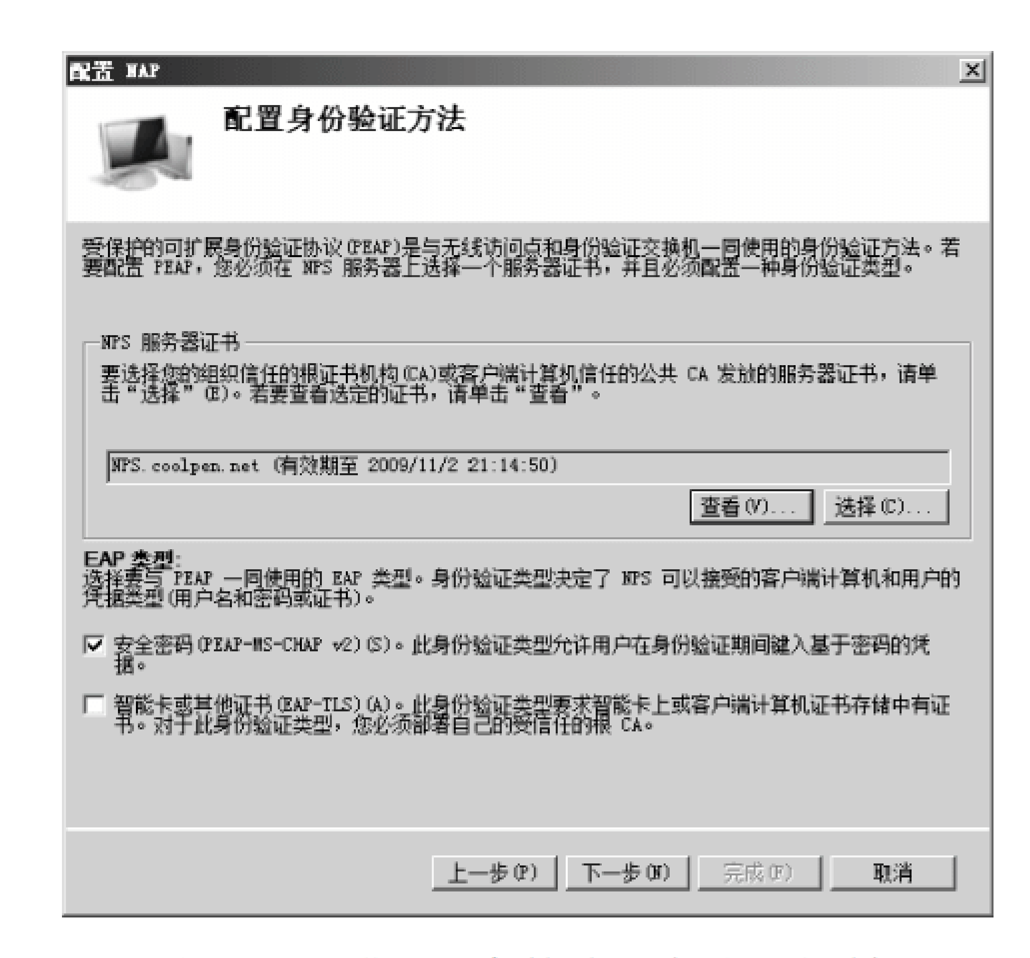


图 11-69　"配置身份验证方法"对话框

(3) 在如图 11-70 所示的“配置虚拟 LAN(VLAN)”对话框中,如果 RADIUS 客户端支持 VLAN,则可以配置 NPS 以向 RADIUS 客户端提供包含更新服务器的受限网络,以及提供完全网络访问权限的组织网络的 VLAN 信息。

(4) 在“配置虚拟 LAN(VLAN)”对话框的“组织网络 VLAN”中,单击“配置”按钮,显示如图 11-71 所示的“虚拟 LAN(VLAN)配置”对话框,在“RADIUS 标准属性”和“供应商特定属性”选项卡中,配置 802.1x 访问点所需的属性,为符合的 NAP 客户端的内网访问指定 ACL 或 VLAN ID。设置完成后,单击“确定”按钮,保存配置即可。



图 11-70 “配置虚拟 LAN(VLAN)”对话框



图 11-71 “虚拟 LAN(VLAN)配置”对话框

(5) 在“配置虚拟 LAN(VLAN)”对话框的“受限网络 VLAN”中,单击“配置”按钮,即可配置“受限网络 VLAN”的相关选项,方法与配置“组织网络 VLAN”选项相同,此处不再赘述。

3. 配置常规网络策略

(1) 打开“网络策略服务器”窗口,依次展开“策略”→“网络策略”选项。在右侧栏中,双击无线或有线网络策略,显示“NAP 802.1x(有线)符合 属性”对话框。在如图 11-72 所示

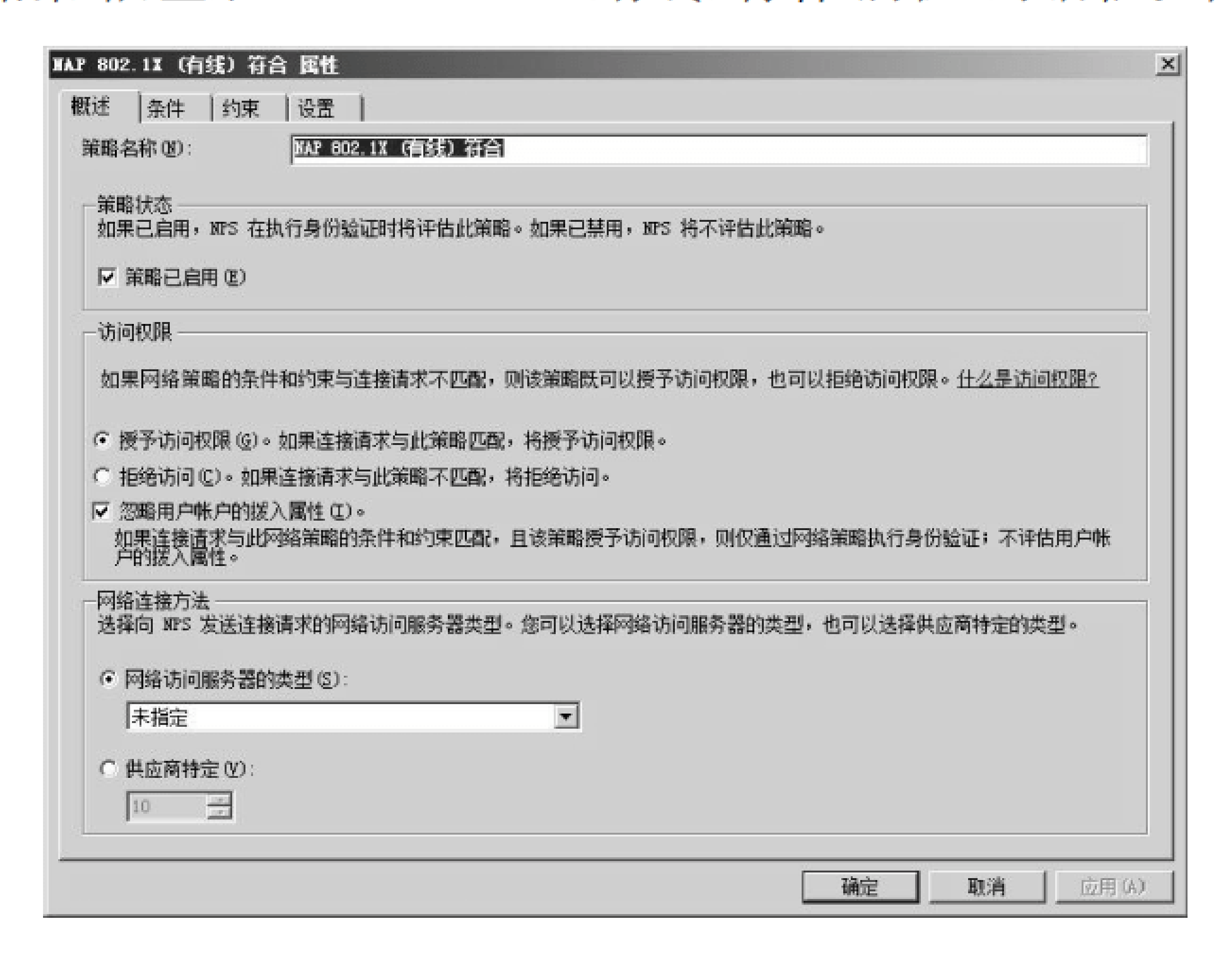


图 11-72 “概述”选项卡

的“概述”选项卡的“网络连接方法”区域中，查看是否设置了“供应商特定”，并根据实际情况选择是否设置。

（2）切换到如图 11-73 所示的“条件”选项卡，查看除了 NAS 端口类型以外是否还有其他条件，并根据实际需要进行设置。

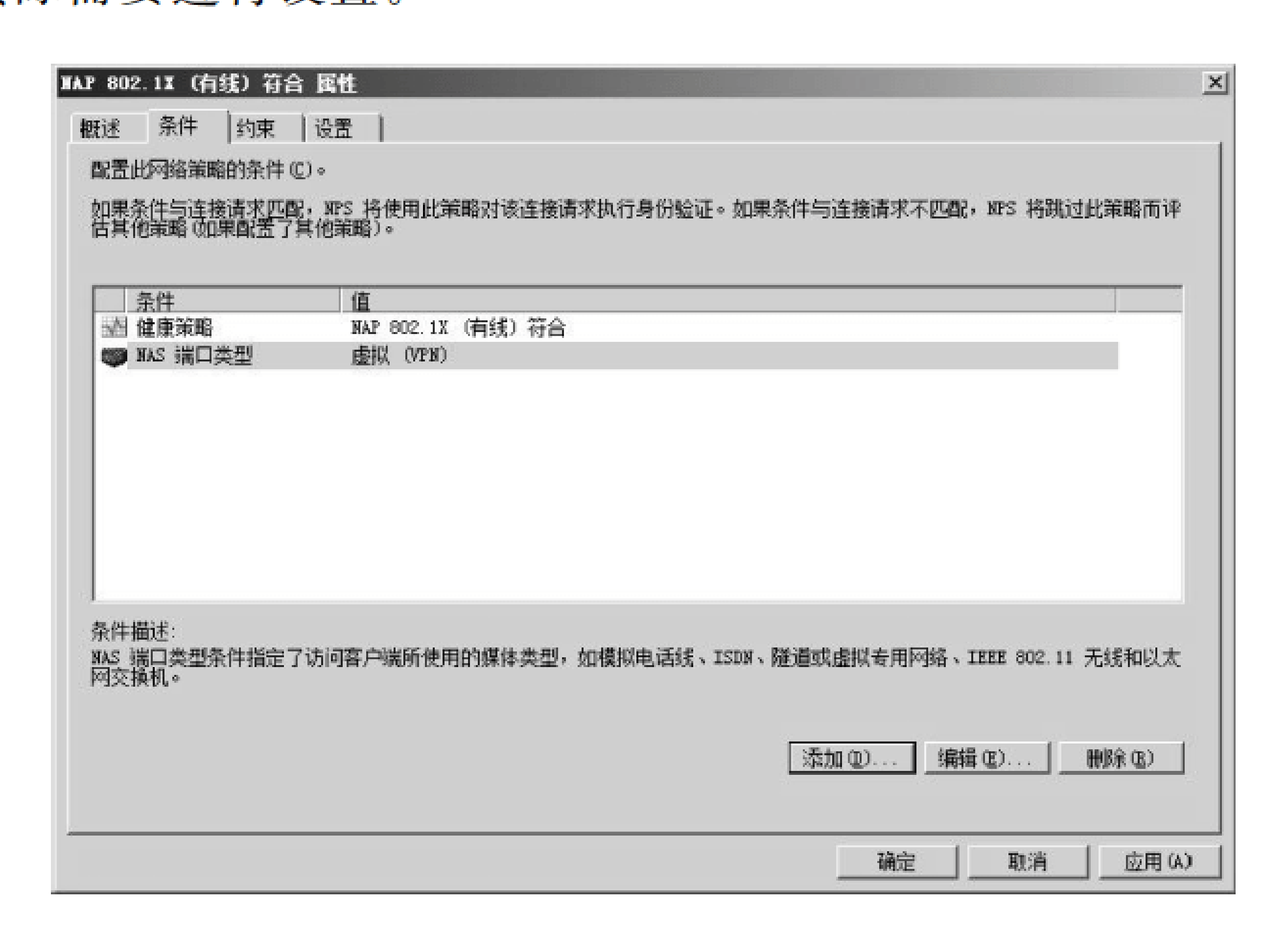


图 11-73　“条件”选项卡

（3）切换到如图 11-74 所示的“约束”选项卡，查看约束列表中的任何设置是否配置了相应值，并根据实际需要进行设置。

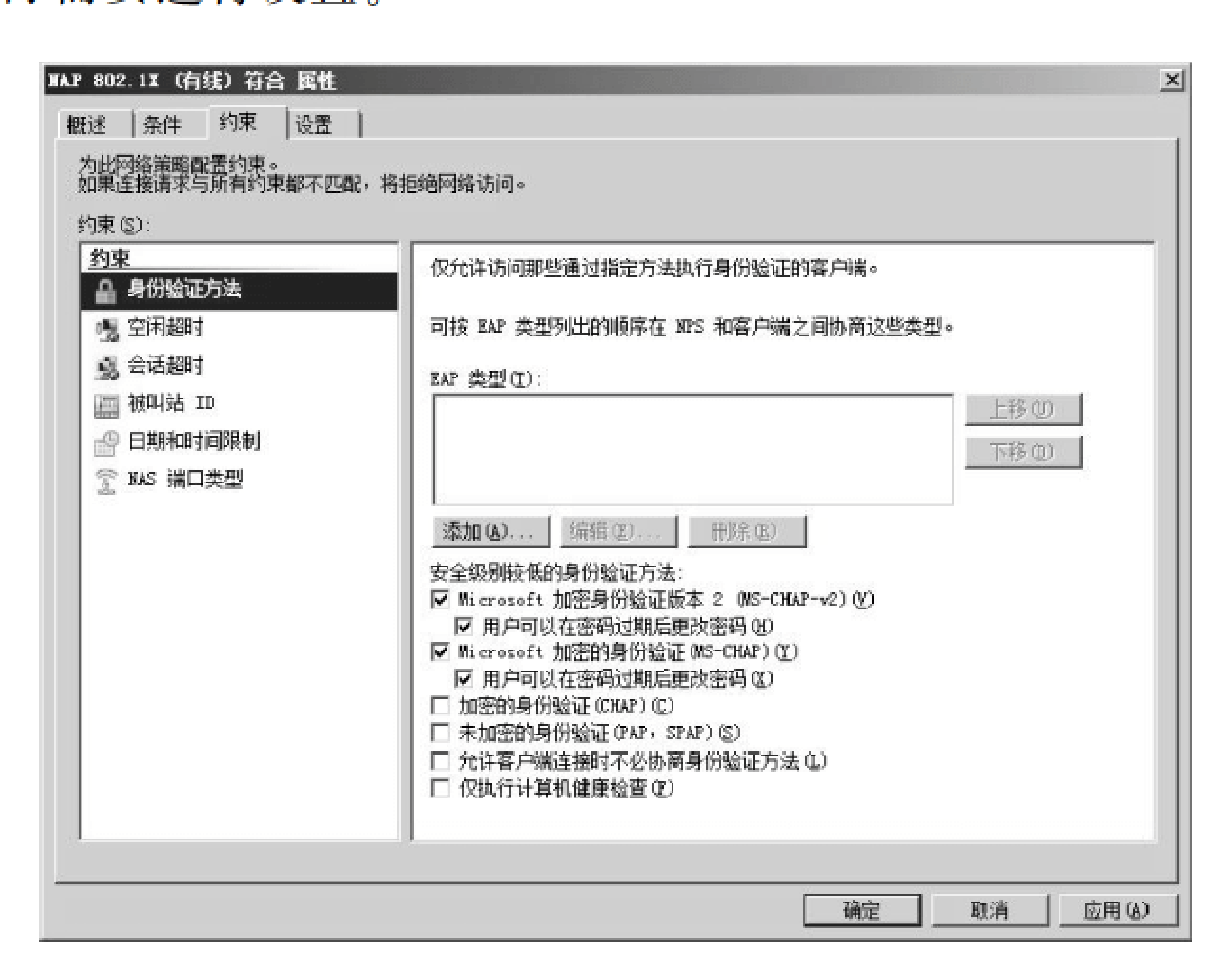


图 11-74　“约束”选项卡

（4）切换到如图 11-75 所示的“设置”选项卡，查看任意其他 RADIUS 标准或供应商指定属性是否配置了 Framed-Protocol 和 Service-Type，并根据实际需要进行设置。

（5）单击“确定”按钮，保存设置即可。

（6）双击“配置 NAP 向导”为符合的 NAP 客户端创建无线或有线网络策略。在“概述”、“条件”、“约束”和“设置”选项卡中，根据步骤（1）～（5）确定的网络策略配置现有无线或有线策略的设置。

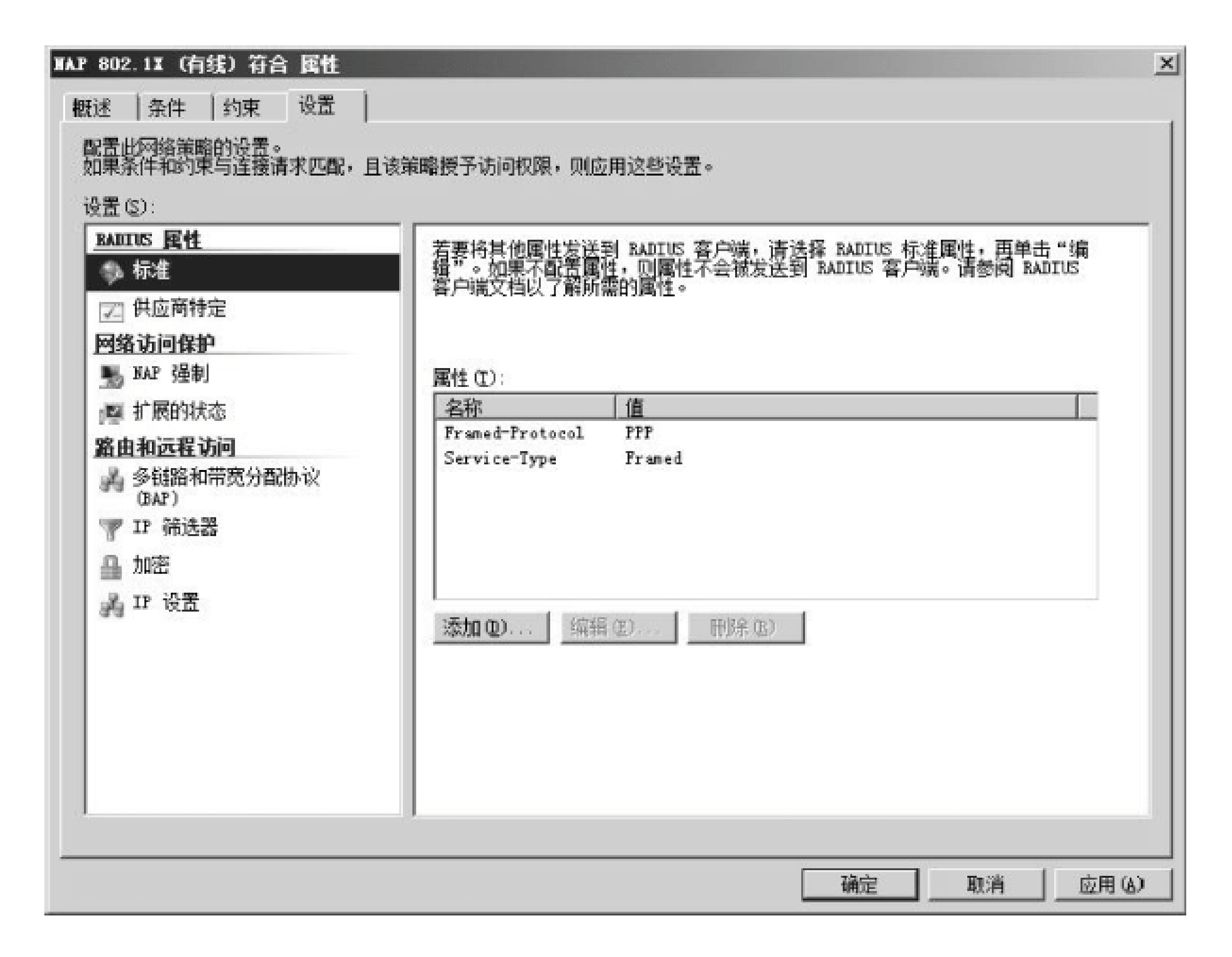


图 11-75 “设置”选项卡

(7) 双击“配置 NAP 向导”为不符合的 NAP 客户端创建的无线或有线网络策略。在“概述”、“条件”、“约束”和“设置”选项卡中，根据步骤(1)～(5)确定的网络策略配置现有无线或有线策略的设置。

(8) 双击“配置 NAP 向导”为不具有 NAP 功能的客户端创建的无线或有线网络策略。在“概述”、“条件”、“约束”和“设置”选项卡中，根据步骤(2)～(5)确定的网络策略配置现有无线或有线策略的设置。

4. 配置报告模式

(1) 打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”选项。在右侧栏中，双击“配置 NAP 向导”，创建不符合的 NAP 客户端的网络策略。

(2) 切换到“设置”选项卡，然后单击“NAP 强制”设置，显示如图 11-76 所示的“NAP 802.1x(有线)不符合 属性”对话框。在网络策略属性对话框的详细面板中，选中“允许完全网络访问”单选按钮。



图 11-76 NAP 强制

(3) 单击“确定”按钮，保存设置即可。

5. 为所要求的健康设置配置健康策略条件

(1) 在“网络策略服务器”管理单元中，依次展开“策略”→“健康策略”选项。

(2) 双击符合和不符合的 NAP 客户端的健康策略，根据健康评估条件和 SHV 的需要进行设置。

在该配置中，创建并配置了 NAP 健康要求策略，但是 NAP 健康策略服务器仍然使用已有的无线或有线连接要求，以及无线或有线访问的网络策略。因此，必须修改连接请求策略的配置，确保 802.1x 强制的新的连接请求策略用于有线或无线连接。

6. 为 802.1x 强制修改连接请求策略

“配置 NAP 向导”创建的无线或有线连接的连接请求策略，要求使用基于 PEAP 的身份验证方法，以及系统健康检查。不使用基于 PEAP 的身份验证方法的 802.1x 客户端的连接尝试，将会被 NAP 健康策略服务器拒绝。使用基于 PEAP 的身份验证方法的，但是不符合健康状态要求的 NAP 客户端，将被 NAP 健康策略服务器定义为不具有 NAP 功能的客户端。

11.4.4　配置 NAP 客户端

尽管可以单独配置 NAP 客户端，但是在活动目录域环境下集中配置 NAP 客户端的最好的方法就是通过组策略设置，主要包括以下步骤。

① 为 PEAP 启用系统健康检查。

② 配置 NAP 客户端设置。

③ 启用 Windows 安全中心(参考 IPSec NAP 客户端的配置)。

④ 配置网络访问保护代理服务的自动启用(参考 IPSec NAP 客户端的配置)。

1. 为 PEAP 启用系统健康检查

尽管已经配置了 NAP 客户端使用 PEAP 身份验证协议，但是如果 PEAP 身份验证协议不启动系统健康检查，NAP 客户端将不会回应系统健康状态的请求。通过组策略扩展，可以为有线和无线网络启用 PEAP 的系统健康检查。

2. 在组策略中为 PEAP 启用系统健康检查

(1) 打开“组策略管理”窗口，右击想要设置的策略名称，在快捷菜单中选择“编辑”选项。打开如图 11-77 所示的“组策略管理编辑器”窗口，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“有线网络(IEEE 802.3)策略”选项。

(2) 双击有线网络策略，显示如图 11-78 所示的“新 Vista 有线网络策略 Properties”对话框。在“策略名”和“描述”文本框中，可根据需要设置策略名称和描述信息。

(3) 切换至“安全”选项卡，单击“属性”按钮，显示如图 11-79 所示的“受保护的 EAP 属性”对话框，选中“启用隔离检查”复选框。

(4) 连续单击“确定”按钮，返回到“组策略管理编辑器”窗口。接下来还需要配置无线连接的相关策略。

(5) 在控制台中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“无线网络(IEEE 802.11)策略”选项。双击创建好的 Vista 无线连接策略，显示如图 11-80 所示的“Vista 无线网络策略 属性”对话框。



图 11-77 展开“有线网络(IEEE 802.3)策略”

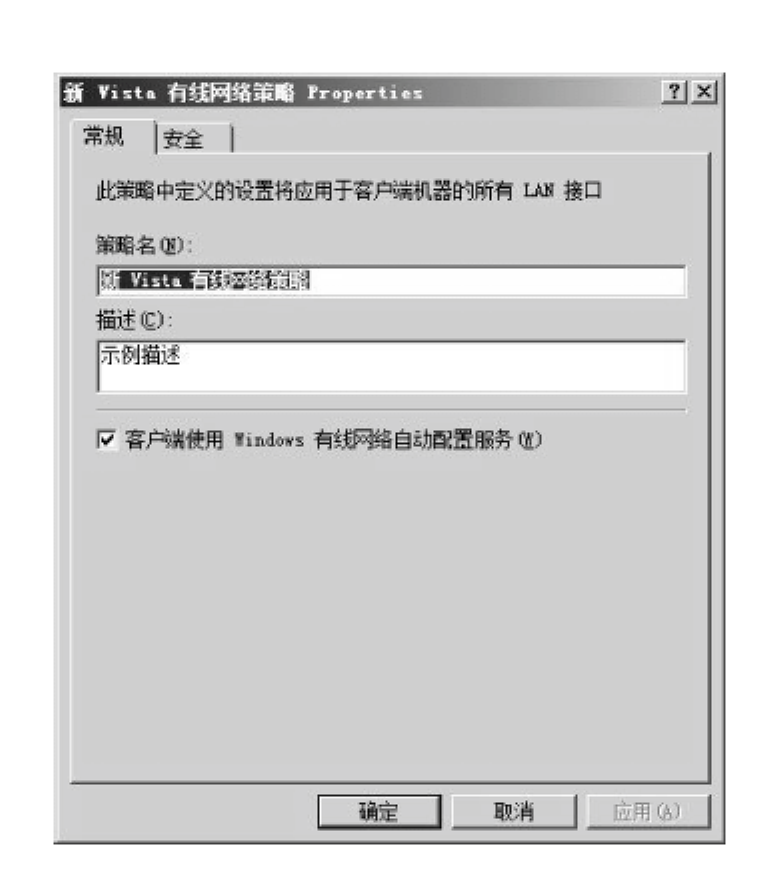


图 11-78 “新 Vista 有线网络策略 Properties”对话框



图 11-79 “受保护的 EAP 属性”对话框

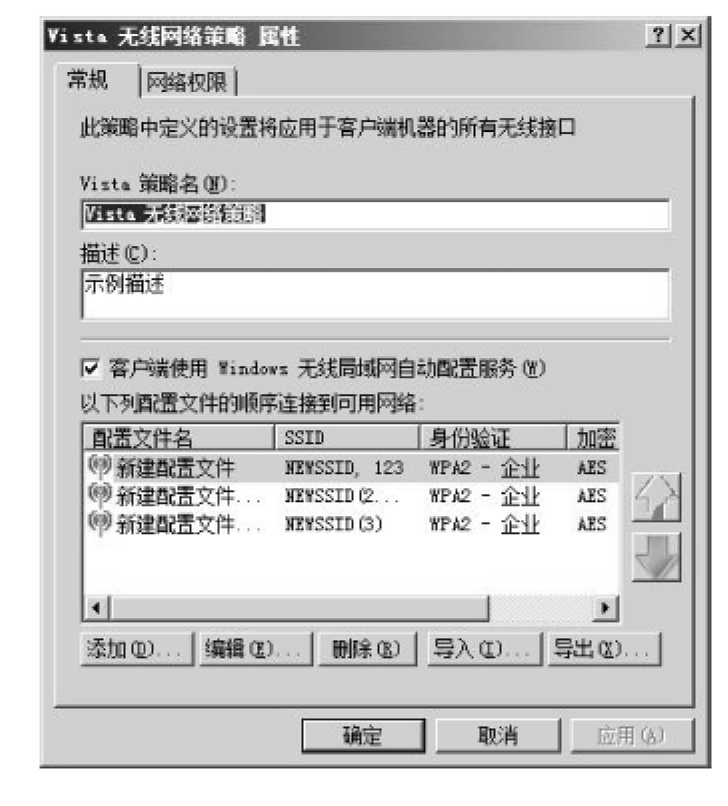


图 11-80 “Vista 无线网络策略 属性”对话框

(6) 双击相应的无线配置文件,显示如图 11-81 所示的“新建配置文件(1)属性”对话框。根据实际需要,设置配置文件的连接信息。

(7) 切换至“安全”选项卡,单击“属性”按钮,显示如图 11-82 所示的“受保护的 EAP 属性”对话框,选中“启用隔离检查”复选框。

(8) 连续单击“确定”按钮,返回到“组策略管理编辑器”对话框。

(9) 双击 XP 无线网络策略,显示如图 11-83 所示的“XP 无线网络策略 属性”对话框。根据需要,设置无线网络策略的名称和描述信息。

(10) 切换至“首选网络”选项卡,在“网络”列表框中,双击相应的无线网络名称,显示如图 11-84 所示的“编辑 NEWSSID 属性”对话框,即可开始编辑其属性设置。



图 11-81 “新建配置文件(1)属性”对话框

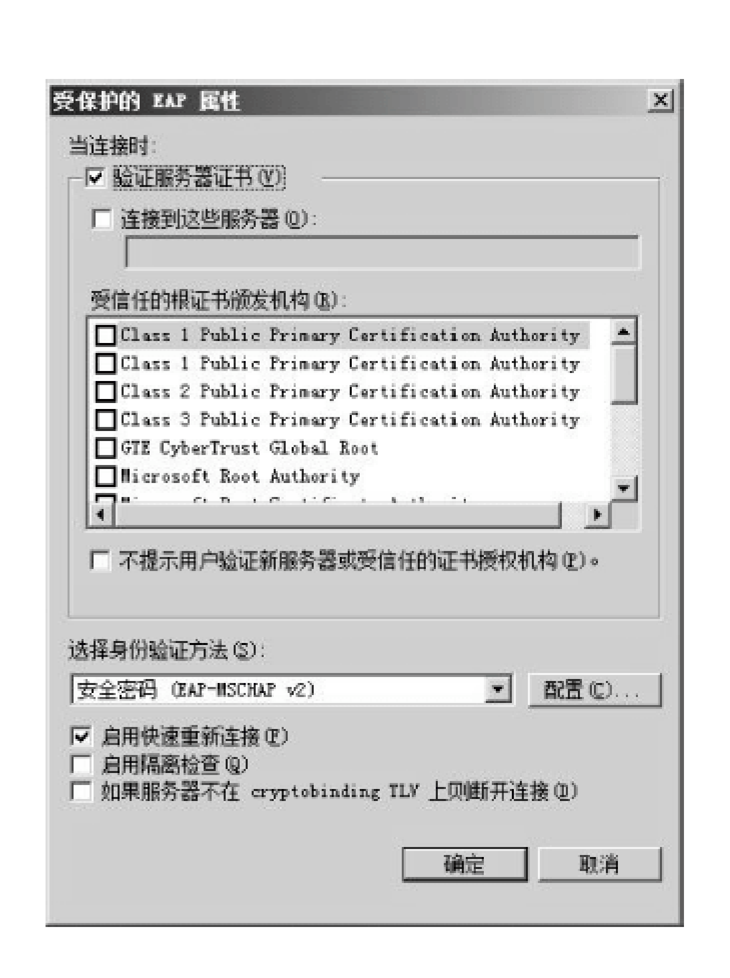


图 11-82 “受保护的 EAP 属性”对话框



图 11-83 “XP 无线网络策略 属性”对话框



图 11-84 “编辑 NEWSSID 属性”对话框

(11) 切换到“IEEE 802.1x”选项卡,单击“设置”按钮,显示如图 11-85 所示的“受保护的 EAP 属性”对话框,选中“启用隔离检查”复选框。

(12) 连续单击“确定”按钮,返回到“组策略管理编辑器”对话框。

提示:因为在运行 Windows XP 的计算机上,没有组策略为有线网络配置 802.1x 身份验证属性,所以必须手动启用 PEAP 的系统健康检查。

3. 配置 NAP 客户端设置

打开“组策略管理”窗口。依次展开“林”→“域”选项,在“链接的组策略对象”面板中,右击适当的组策略对象,在快捷菜单中选择“编辑”选项,打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“网络访问保护”→“NAP 客户端配置”选项。

在控制台中,单击“强制客户端”,在右侧栏中,双击“EAP 隔离强制客户端”图标,显示如图 11-86 所示的“EAP 隔离强制客户端 属性”对话框。选中“启用此强制客户端”复选框,单击“确定”按钮,保存设置。

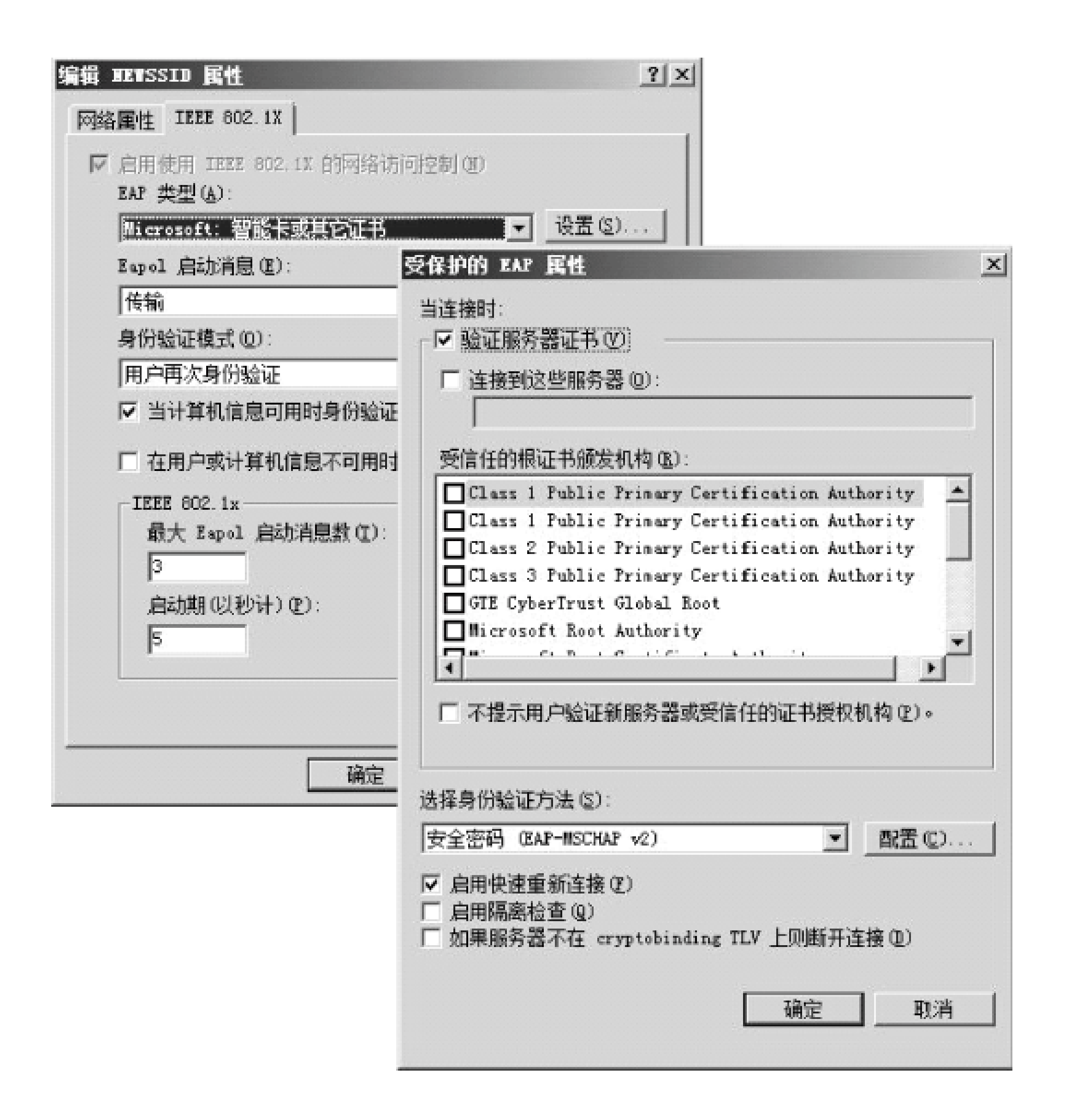


图 11-85 “受保护的 EAP 属性”对话框

对于运行 Windows XP SP3 的计算机，在控制台中，依次展开“计算机配置”→“管理模板”→“Windows 组件”→“网络访问保护”选项。然后在右侧栏中，双击“允许网络访问保护客户端支持 802.1x 强制客户端组件”图标，显示如图 11-87 所示的“允许网络访问保护客户端支持 802.1x 强制客户端组件 属性”对话框。在“设置”选项卡中，选中“已启用”单选按钮，然后单击“确定”按钮，保存设置即可。



图 11-86 “EAP 隔离强制客户端 属性”对话框

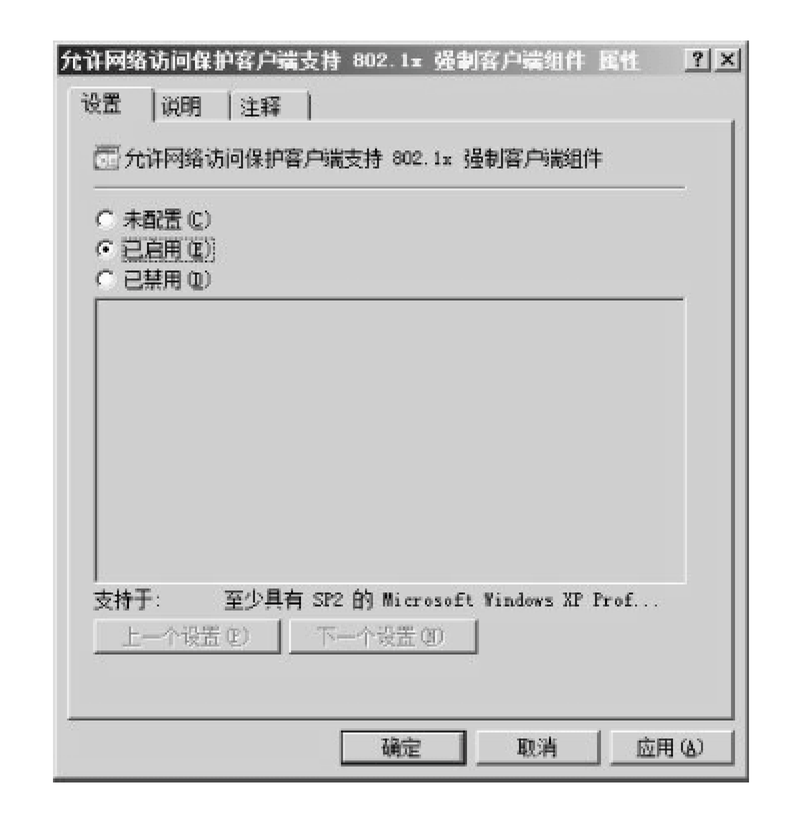


图 11-87 “允许网络访问保护客户端支持 802.1x 强制客户端组件 属性”对话框

11.5 配置 VPN 强制

对 VPN 强制的工作过程有所了解之后，即可开始在网络中部署 VPN 强制。需要注意的是，某些环节对系统或网络策略安全性配置要求比较高，如果服务器分配不够合理，则可

能导致应用故障。如果条件允许，建议为每台服务器角色选择单独的服务器，以免由于彼此之间的系统环境需求不同，而导致兼容问题。该企业网络中将 VPN 服务器与 NPS 服务器规划在同一台计算机上。

11.5.1 为 VPN 服务器配置 EAP 身份验证

如果用户没有为远程访问 VPN 连接使用基于 EAP 的身份验证方法，则用户必须配置基于 Windows Server 2008 的 VPN 服务器使之运行基于 EAP 的身份验证。

(1) 在"路由和远程访问"窗口，右击路由和远程访问服务器的名称，在快捷菜单中选择"属性"选项，显示"VPN(本地) 属性"对话框。单击"安全"标签切换至如图 11-88 所示的"安全"选项卡。由于安装了 NPS 服务器，必须使用它进行身份验证和记账。

(2) 单击"身份验证方法"按钮，显示如图 11-89 所示的"身份验证方法"对话框，选中"可扩展的身份验证协议(EAP)"复选框。



图 11-88 "安全"选项卡

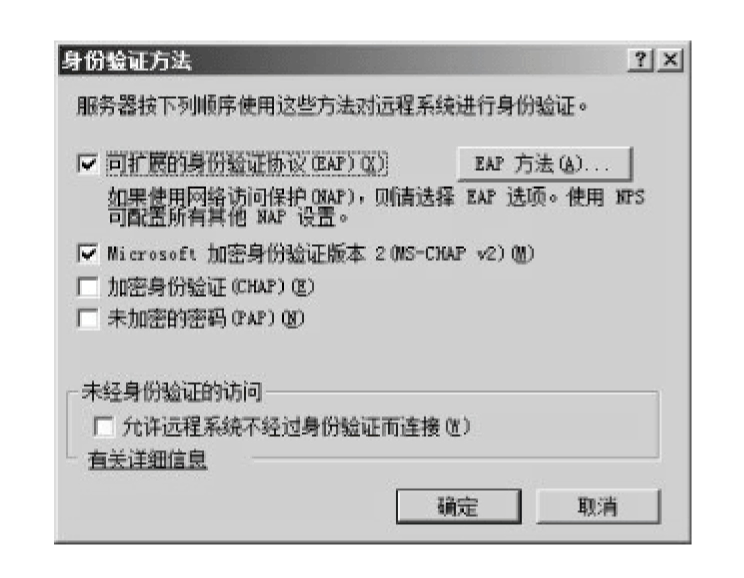


图 11-89 "身份验证方法"对话框

(3) 连续两次单击"确定"按钮，保存配置即可。

11.5.2 配置 NAP 健康策略服务器

VPN 强制的 NAP 健康策略服务器，与远程访问 VPN 身份验证所使用的 NPS RADIUS 服务器相同。为了配置 NAP 健康策略服务器，用户必须对现有 NPS 服务器进行如下配置。

① 申请计算机验证证书。

② 安装和配置 SHV。

③ 配置 RADIUS 服务器设置。

④ 配置 VPN 强制的健康要求策略。

1. 申请计算机验证证书

(1) 在 NPS 服务器上，单击"开始"按钮，在"开始搜索"文本框中输入 mmc 并按 Enter 键，打开"控制台"窗口，依次选择"文件"→"添加或删除管理单元"选项，显示如图 11-90 所示的"添加或删除管理单元"对话框，在"可用的管理单元"列表中，选择"证书"单元。

(2) 单击"添加"按钮，显示如图 11-91 所示的"证书管理单元"对话框，选中"计算机账

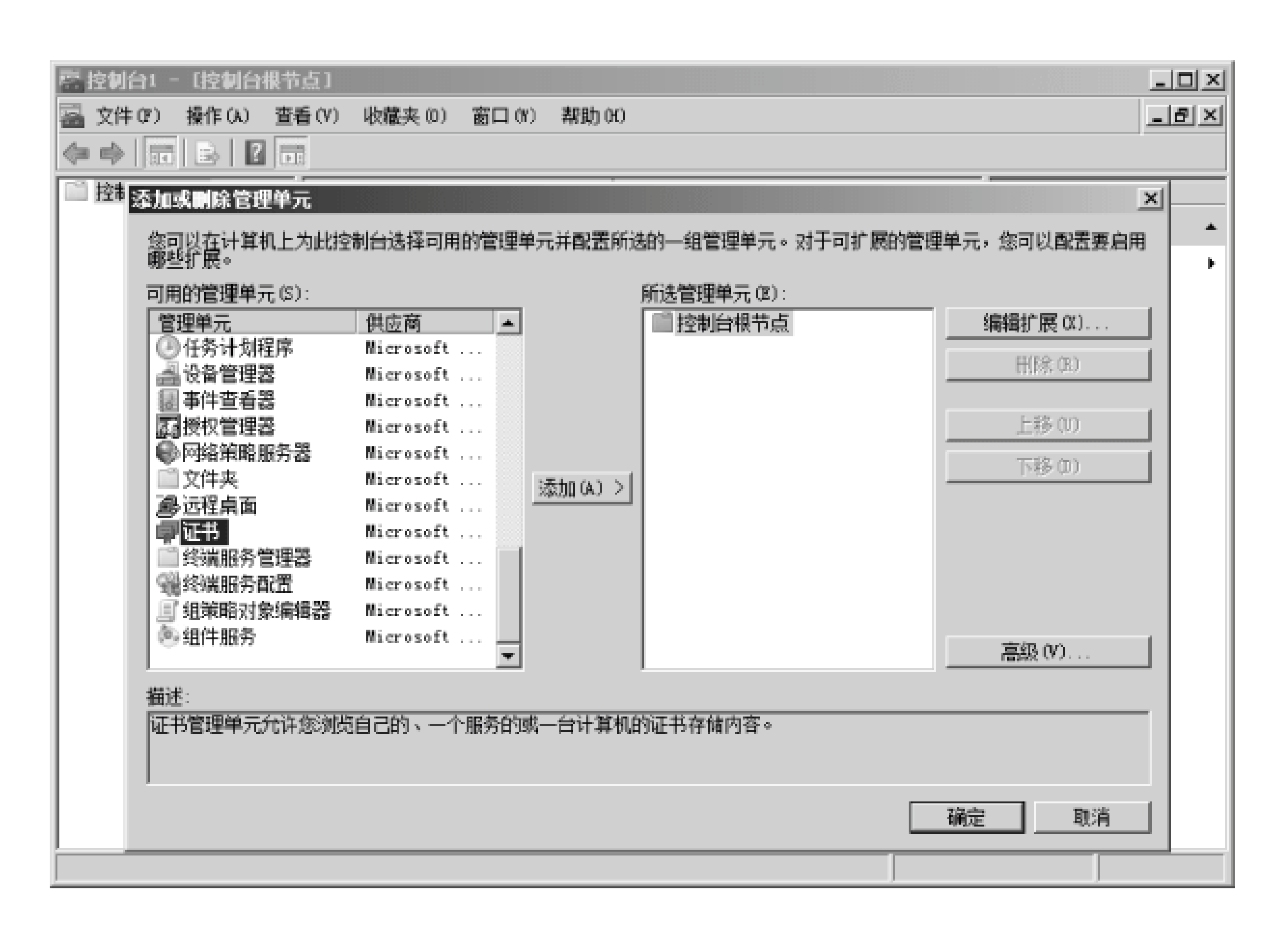


图 11-90 “添加或删除管理单元”对话框

户”单选按钮。

(3) 单击“下一步”按钮，在“选择计算机”对话框中，选中“本地计算机”单选按钮。依次单击“完成”按钮和“确定”按钮，返回“控制台”窗口。在“控制台”窗口中，依次展开“证书(本地计算机)”→“个人”选项，右击“个人”并依次选择“所有任务”→“申请新证书”选项，显示如图 11-92 所示的“在您开始前”对话框。



图 11-91 “证书管理单元”对话框



图 11-92 “在您开始前”对话框

(4) 单击“下一步”按钮，显示如图 11-93 所示的“申请证书”对话框，选中“计算机”复选框。

(5) 单击“注册”按钮，开始向网络中的 CA 提交证书申请，稍等即可成功。单击“完成”按钮，返回“控制台”窗口，如图 11-94 所示。

2. 创建 VPN 强制策略

(1) 在 NPS 服务器上，打开“网络策略管理器”窗口。单击 NPS，在“标准配置”下拉列表框中选择“网络访问保护(NAP)”选项。单击“配置 NAP”链接，显示如图 11-95 所示的“选择与 NAP 一起使用的网络连接方法”对话框。在“网络连接方法”中，选择“虚拟专用网络(VPN)”，在“策略名称”文本框中输入对应的名称，建议使用默认名称。

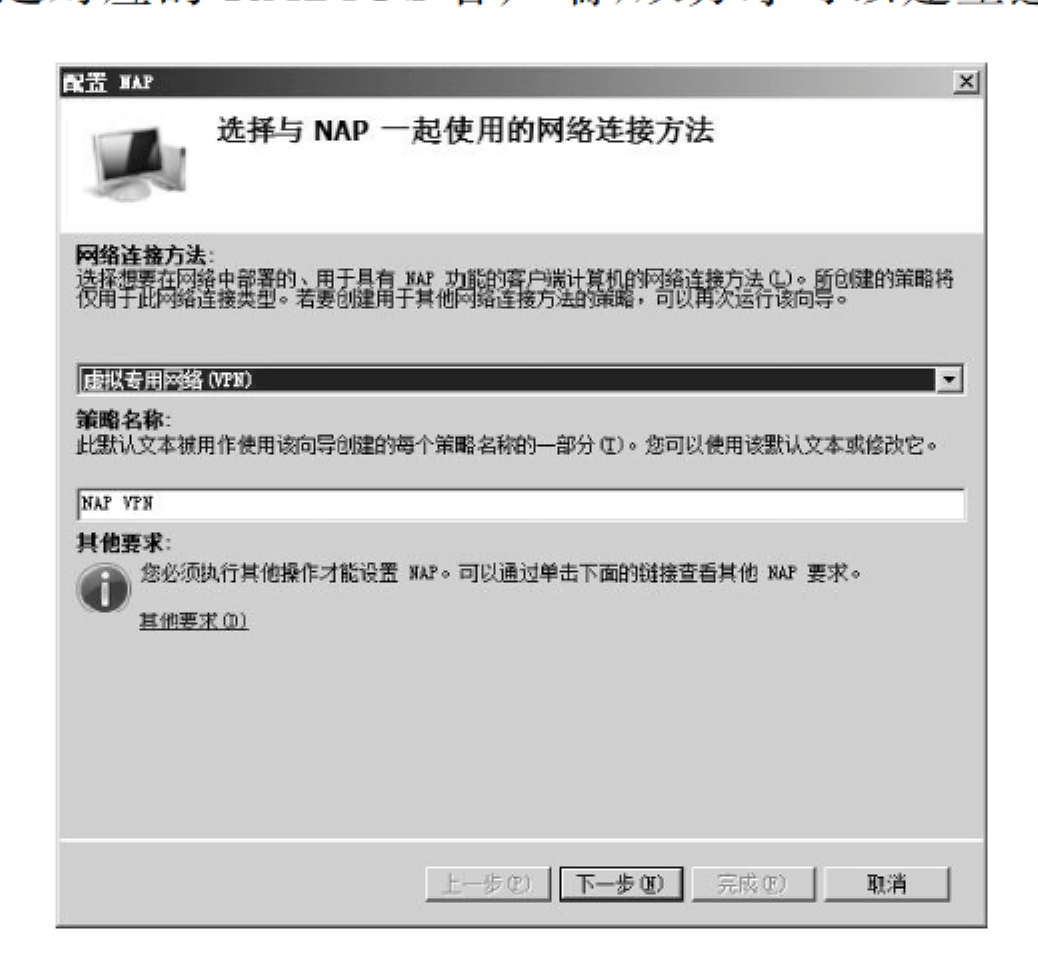


图 11-93 “申请证书”对话框



图 11-94 “控制台”窗口

(2) 单击“下一步”按钮，显示如图 11-96 所示的“指定 NAP 强制服务器运行 VPN 服务器”对话框，由于 NAP 健康策略服务器已经是一台 RADIUS 服务器，本例中配置 VPN 服务器时，已经将 RADIUS 服务器指向该服务器。需要注意的是，必须在该服务器上设置与之对应的 RADIUS 客户端，双方才可以建立连接。



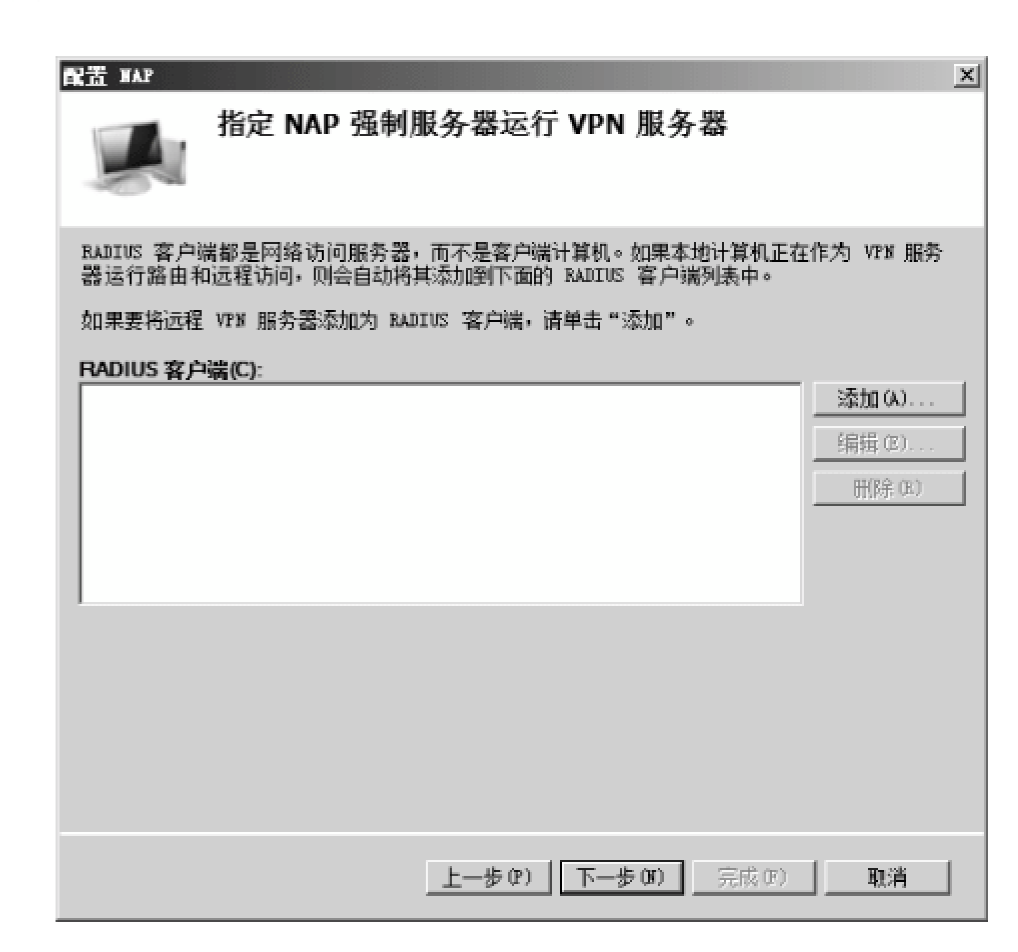


图 11-95 “选择与 NAP 一起使用的网络连接方法”对话框

图 11-96 “指定 NAP 强制服务器运行 VPN 服务器”对话框

提示：如果在此之前，管理员在 NPS→“RADIUS 服务器和客户端”中设置了指向 VPN 服务器的 RADIUS 客户端，则将显示在“RADIUS 客户端”列表中。

(3) 单击“添加”按钮，显示如图 11-97 所示的“新建 RADIUS 客户端”对话框，在“友好名称”文本框中，设置适当的名称，在“地址”文本框中，输入 VPN 服务器的 IP 地址。“共享机密”的方式必须与 VPN 服务器相匹配。

(4) 单击“确定”按钮，返回“指定 NAP 强制服务器运行 VPN 服务器”对话框。单击“下一步”按钮，显示如图 11-98 所示的“配置用户组和计算机组”对话框，根据需要配置组。如果不选择，则将对所有计算机组和用户组有效。

(5) 单击“下一步”按钮，显示如图 11-99 所示的“配置身份验证方法”对话框，为 PEAP 身份验证选择 NPS 所使用的计算机证书，即上述操作中申请的验证证书。根据需要选中





图 11-97 “新建 RADIUS 客户端”对话框



图 11-98 “配置用户组和计算机组”对话框

“安全密码(PEAP-MS-CHAP v2)”或者“智能卡或其他证书(EAP-TLS)”复选框。需要注意的是，VPN 服务器、NPS 和客户端必须设置完全相同的身份验证方式，否则无法建立连接。如果默认没有使用该证书，则可以单击“选择”按钮，显示“选择证书”对话框，确认为所需证书即可。

(6) 单击“下一步”按钮，显示如图 11-100 所示的“指定 NAP 更新服务器组和 URL”对话框。更新服务器组的主要作用就是对未通过健康策略审查的被隔离客户端进行“补救”，通常包括 WSUS 服务器、网络防病毒服务器等。除此之外，也可以根据健康策略的审查重点不同，而不设置更新服务器组，例如仅检测网络防火墙状态。在这里单击“新建组”按钮，可以配置更新服务器组。



图 11-99 “配置身份验证方法”对话框

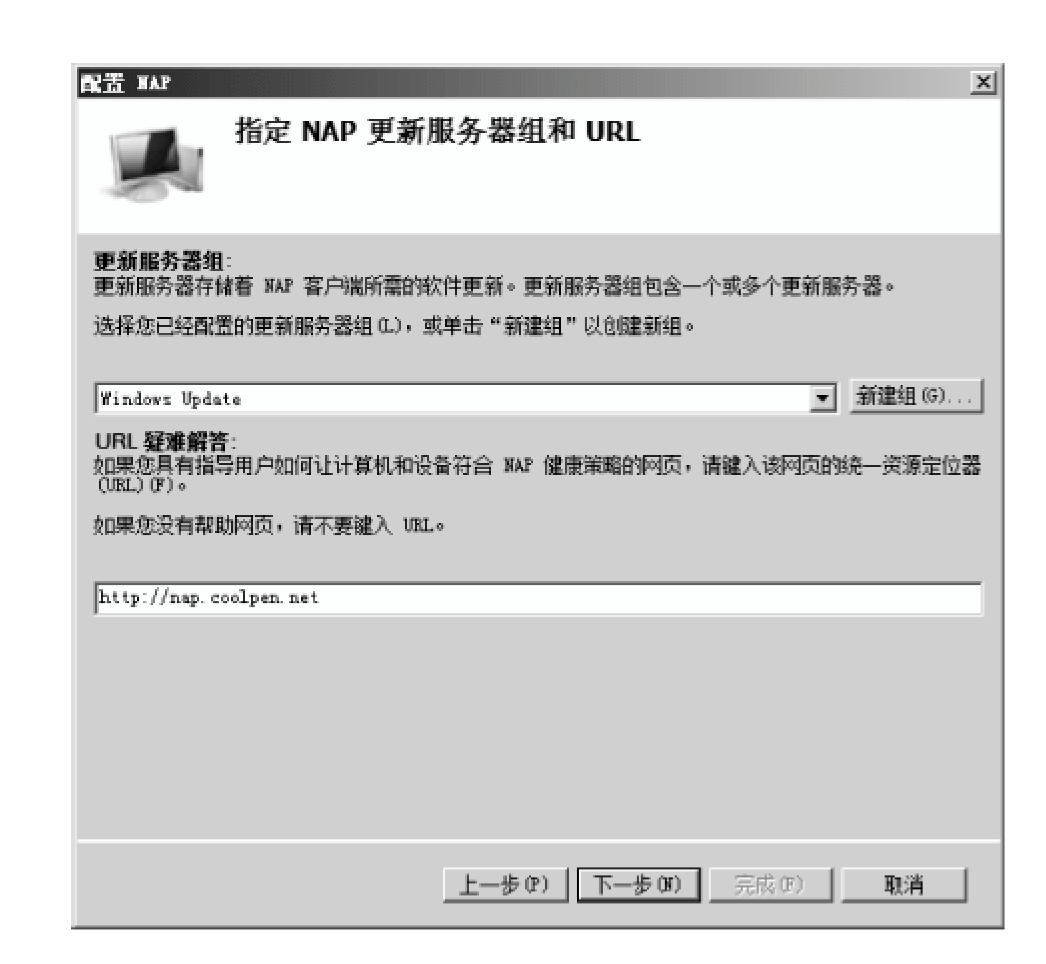


图 11-100 “指定 NAP 更新服务器组和 URL”对话框

(7) 单击“下一步”按钮，显示如图 11-101 所示的“定义 NAP 健康策略”对话框，选择 VPN 强制需要评估的 SHV，根据需要选择“启用客户端计算机的自动更新”选项。选中“允

许对不具有 NAP 功能的客户端计算机的完全网络访问权限”单选按钮，即可使用户想要不支持 NAP 功能的客户端拥有受限访问。选中“启用客户端计算机的自动更新”复选框，则当由于客户端计算机的自动更新为开启而未通过策略审核被隔离时，将自动启动客户端的自动更新设置。

(8) 单击“下一步”按钮，显示如图 11-102 所示的“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框。

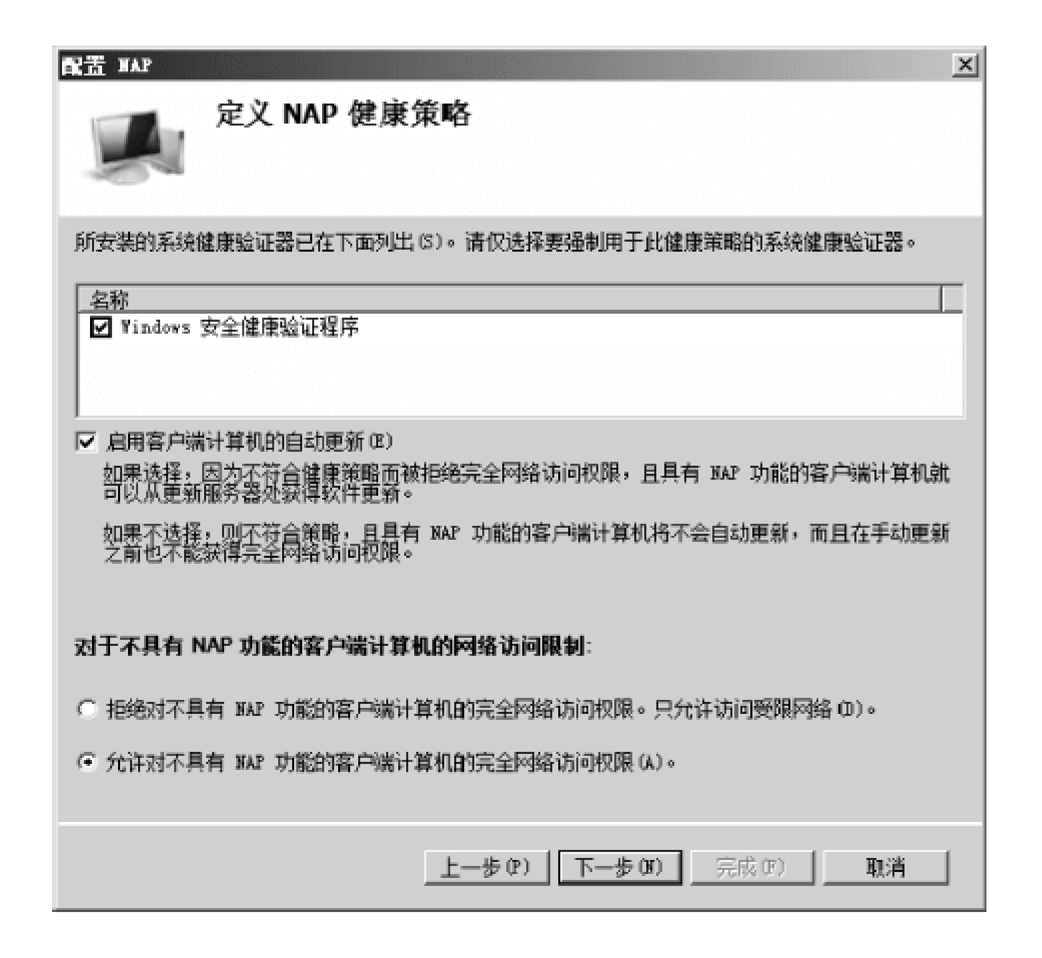


图 11-101 “定义 NAP 健康策略”对话框



图 11-102 “正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框

(9) 单击“完成”按钮，关闭“配置 NAP”向导。

“配置 NAP”向导创建的连接请求策略、健康策略和网络策略位于各自顺序列表的底部，直到用户删除或改变现有远程访问 VPN 网络策略，“配置 NAP”向导创建的网络策略才会用于基于 VPN 的远程访问连接的身份验证或健康评估。

提示：为了确保“配置 NAP”向导产生的策略是正确无误的，应在“策略”的“连接请求策略”、“健康策略”和“网络策略”中，一一检查每条策略的执行顺序、条件、约束和设置等。

3. 安装和配置 SHV

SHV 必须安装在 NAP 健康策略服务器上，进行健康策略评估。NPS 服务包含 Windows 安全健康验证程序 SHV，来指定运行 Windows Vista 或 Windows XP SP3 的 NAP 客户端的 Windows 安全中心设置，包括防火墙、自动更新、防病毒程序、防间谍软件等审核对象。安装其他 SHV 的方法将取决于 SHV 供应商，可以通过供应商主页下载或者运行供应商提供的 CD-ROM 中的安装程序进行安装。配置方法与其他类型强制相同，详细操作参考本章“配置 IPSec 强制”中的相关内容。

4. 为 RADIUS 客户端配置 NAP 支持

NAP 健康策略服务器已经为远程访问 VPN 连接配置完成。对于 VPN 连接，用户必须在 VPN 相应的 RADIUS 客户端属性对话框中，选中“RADIUS 客户端支持 NAP”复选框。用户也可以从“网络策略管理器”管理单元的“RADIUS 客户端”节点中更改 RADIUS 客户端的属性。由于 VPN 强制配置将使用报告模式，不符合的 NAP 客户端拥有不受限的访问，所以用户在启用强制模式之前，可能需要更改 NAP 健康策略服务器的登录入站

请求。



图 11-103 “VPN 属性”对话框

在“网络策略服务器”窗口中，依次展开“NPS(本地)”→“RADIUS 客户端和服务器”→“RADIUS 客户端”选项。右击名称为 VPN 的 RADIUS 客户端，选择快捷菜单中的“属性”选项，显示如图 11-103 所示的“VPN 属性”对话框，选中“RADIUS 客户端支持 NAP”复选框。

11.5.3 配置 NAP 客户端

由于 VPN 客户端建立到 VPN 服务器之间的连接之前，需要先通过 NPS 服务器的健康评估，所以与常规 VPN 客户端配置有所不同。配置 NAP 客户端的基本步骤如下。

① 下载客户端计算机证书。

② 安装 SHA。

③ 创建和配置 VPN 客户端。

④ 通过组策略配置可管理的 NAP 客户端。

1. 下载验证证书

客户端计算机必须登录域中的 CA，获取所需的验证证书。

(1) 打开 IE 浏览器，按照 http://CA 服务器/certsrv 方式登录 CA，显示如图 11-104 所示的窗口。

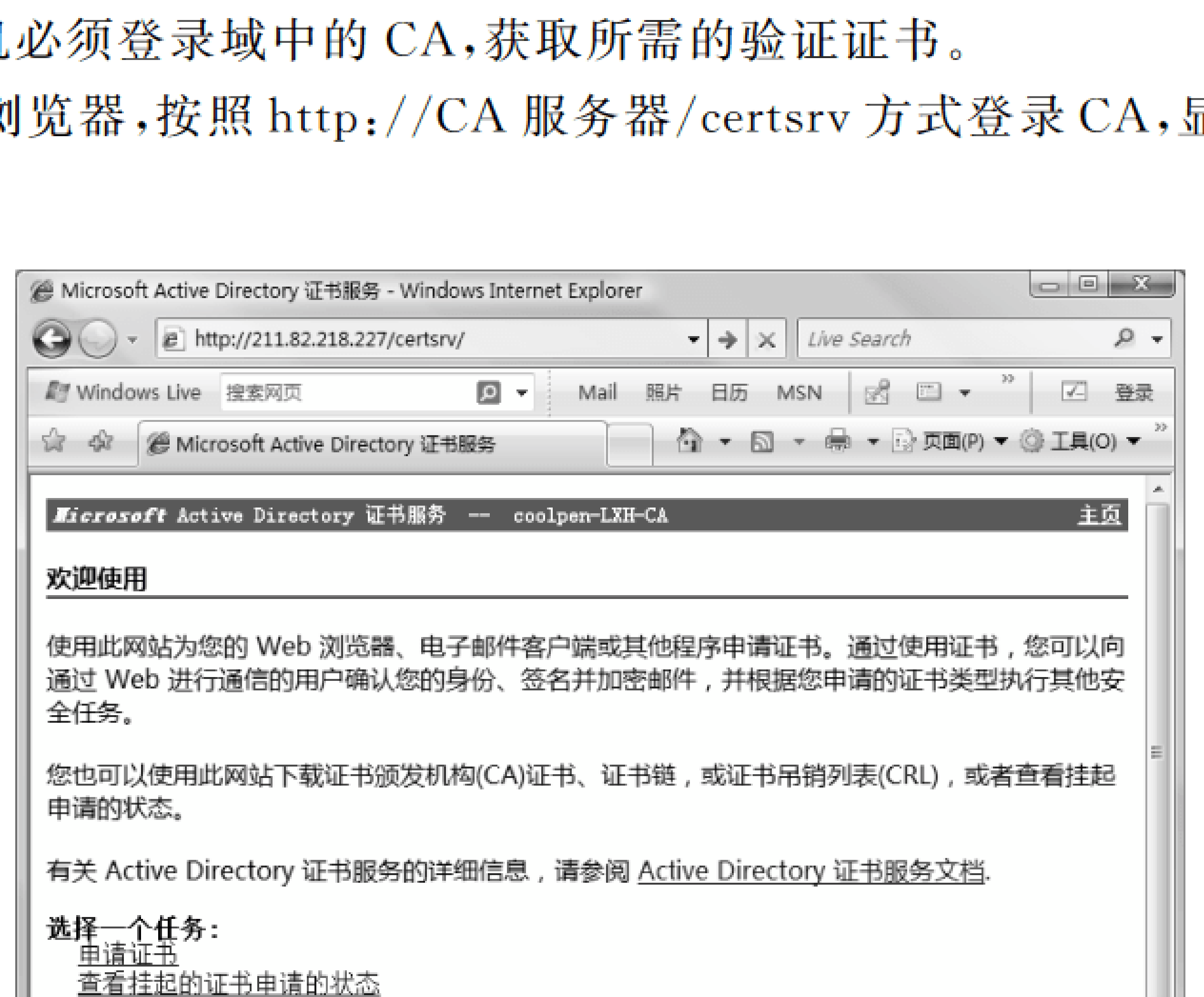


图 11-104 登录证书服务器

注意：集成在域控制器上的 CA，默认情况下，已禁止“允许匿名访问”方式，此时可以联系域管理员，登录证书服务器，并在 IIS 管理器中，启用 CA 站点以及 Certsrv 目录的“允许匿名访问”身份验证方式。

(2) 单击“下载 CA 证书、证书链或 CRL”链接，显示如图 11-105 所示的“下载 CA 证书、

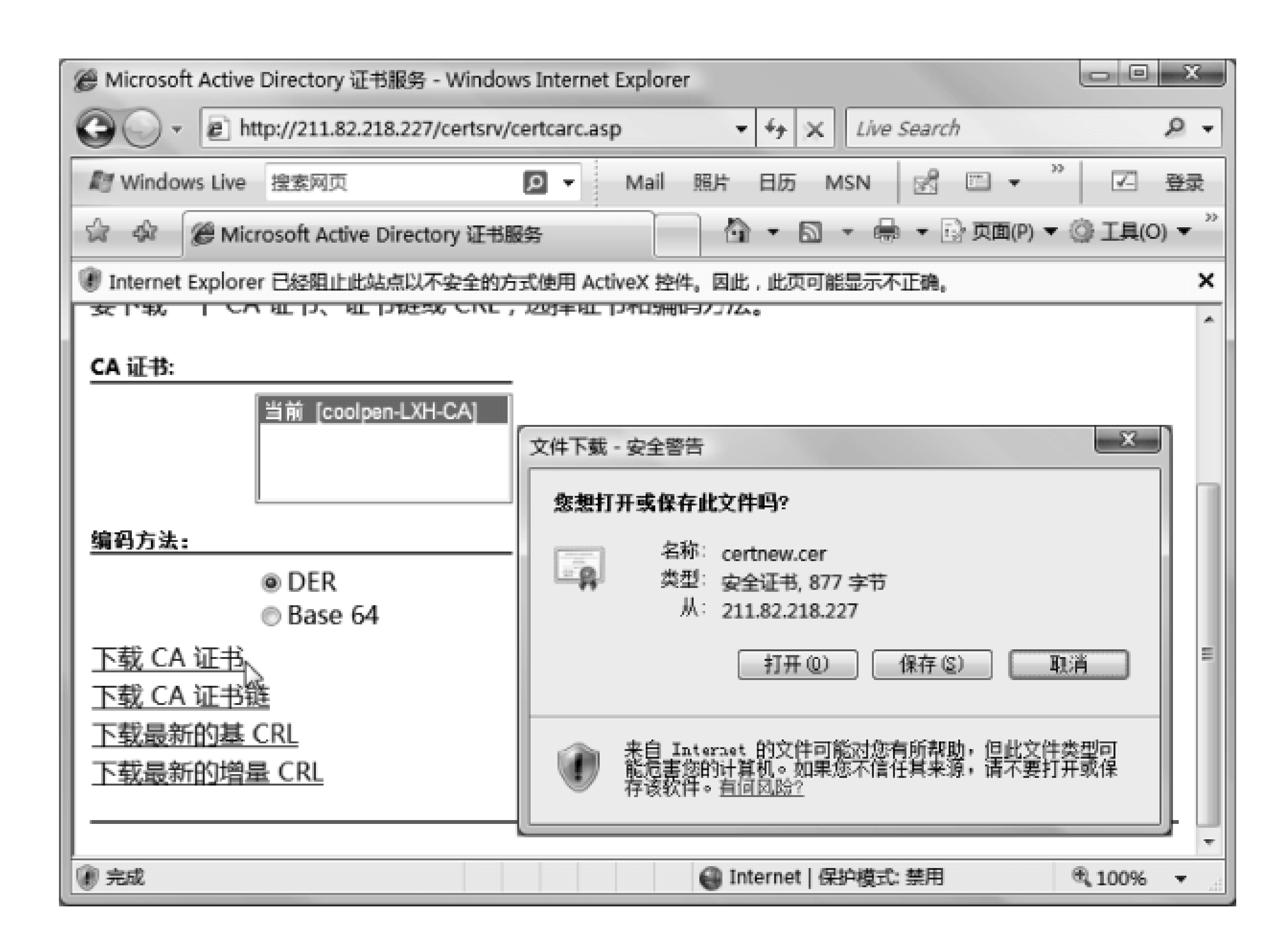


图 11-105 “文件下载-安全警告”对话框

证书链或 CRL”窗口。单击“下载 CA 证书”链接，显示“文件下载-安全警告”对话框。

（3）可以单击“保存”按钮，先将证书保存到本地计算机，然后再安装到相应的目录下，也可以单击“打开”按钮，直接开始安装。

安装过程中需要注意的是，在“证书存储”步骤，需要选中“将所有的证书放入下列存储”单选按钮，并单击“浏览”按钮，打开“选择证书存储”对话框，选择“受信任的根证书颁发机构”目录，如图 11-106 所示。

2．创建和配置 VPN 客户端

VPN 客户端连接的创建比较简单，详细操作过程，参考本章中的相关介绍，此处不再赘述。配置 VPN 强制时，应注意客户端身份验证协议是否正确，确保与 VPN 服务器完全一致，否则将无法建立连接。

（1）在“网络连接”窗口中，右击创建的 VPN 连接，选择快捷菜单中的“属性”选项，打开“coolpen 属性”对话框。切换至“安全”选项卡，选中“高级（自定义设置）”单选按钮，如图 11-107 所示。

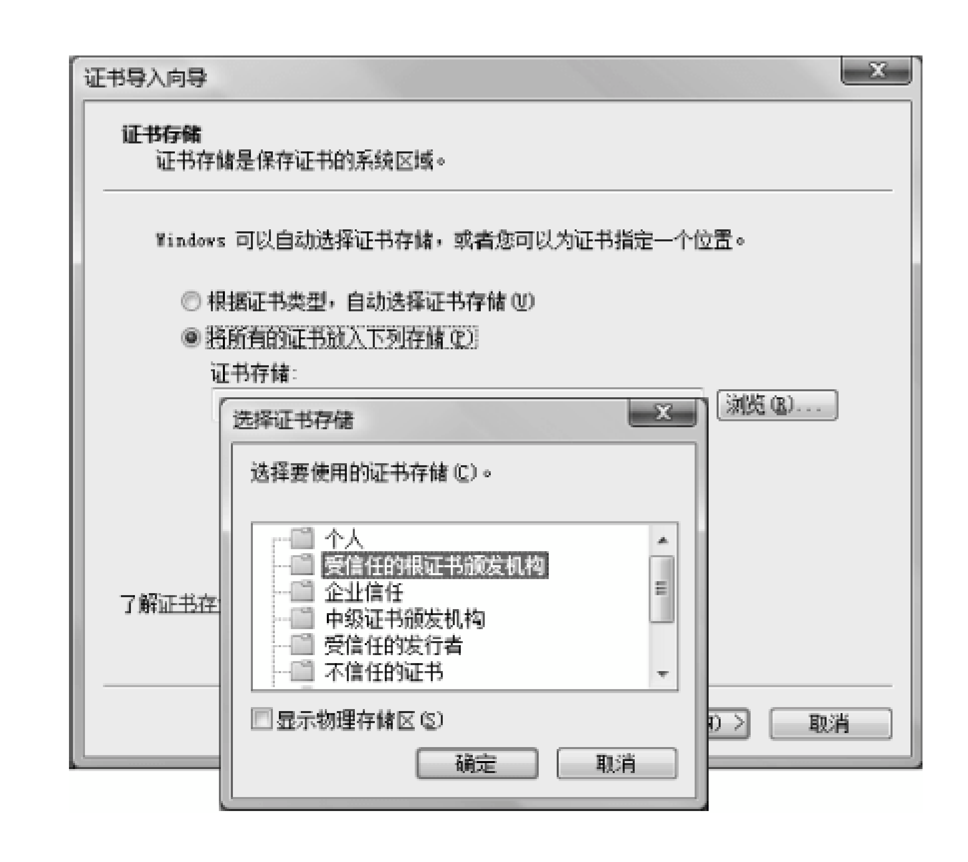


图 11-106 “选择证书存储”对话框



图 11-107 “安全”选项卡

(2) 单击“设置”按钮,显示如图 11-108 所示的“高级安全设置”对话框,在“数据加密”下拉列表框中选择“需要加密(如果服务器拒绝将断开连接)”选项,选中“使用可扩展的身份验证协议(EAP)”单选按钮,并选择下拉列表框中的“受保护的 EAP”选项。

(3) 单击“属性”按钮,显示如图 11-109 所示的“受保护的 EAP 属性”对话框,取消“连接到这些服务器”复选框。选中“验证服务器证书”复选框,在“受信任的根证书颁发机构”列表框中,会发现已经安装的证书颁发机构。在“选择身份验证方法”下拉列表框中,选择“安全密码”选项。选中“启用隔离检查”复选框。



图 11-108 “高级安全设置”对话框

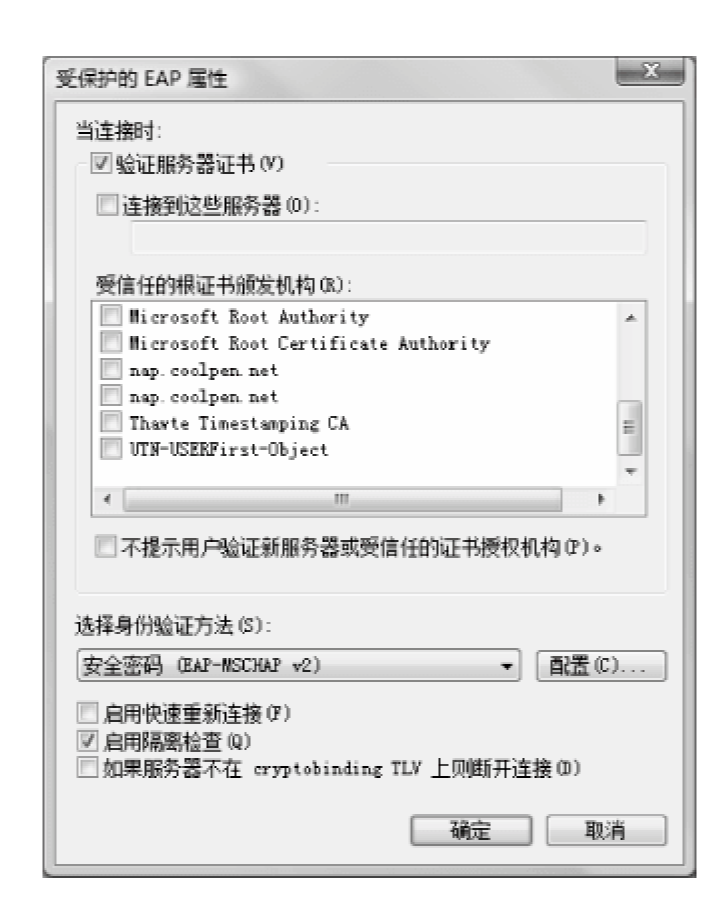


图 11-109 “受保护的 EAP 属性”对话框

3. 通过组策略配置 NAP 客户端

当服务器配置了 NPS 策略以后,还需要对客户端计算机进行一定的配置,包括启用安全中心、启用 NAP 客户端、启用代理服务等。这样,才能实现对客户端计算机的网络访问保护。虽然用户可以在自己的计算机上进行配置,但为了提高效率,通常利用组策略完成,使客户端用户登录时自动设置计算机的设置,完成 NAP 保护功能。

(1) 创建组策略

① 以域管理员身份登录到域控制器,打开“Active Directory 用户和计算机”控制台,创建一个组织单位,并将 VPN 用户账户移动到该组织单位中。依次选择“开始”→“管理工具”→“组策略管理”选项,打开“组策略管理”控制台,依次展开“林:coolpen.net”→“域”→coolpen.net 选项,如图 11-110 所示。

② 选择欲配置 VPN 策略的组织单位,右击并选择快捷菜单中的“在这个域中创建 GPO 并在此处链接”选项,显示如图 11-111 所示的“新建 GPO”对话框。在“名称”文本框中为该策略输入一个名称。

③ 单击“确定”按钮,一个组策略创建完成。右击该组策略并选择快捷菜单中的“编辑”按钮,打开如图 11-112 所示的“组策略管理编辑器”窗口。

(2) 启用安全中心

在“组策略管理编辑器”窗口中,依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“安全中心”选项。选择“启用安全中心(仅限域 PC)”策略,右击并选择快捷菜单中的“属性”选项,打开“启用安全中心(仅限域 PC)属性”对话框。选中“已启用”单选按钮,如图 11-113 所示。最后,单击“确定”按钮保存即可。



图 11-110　“组策略管理”控制台



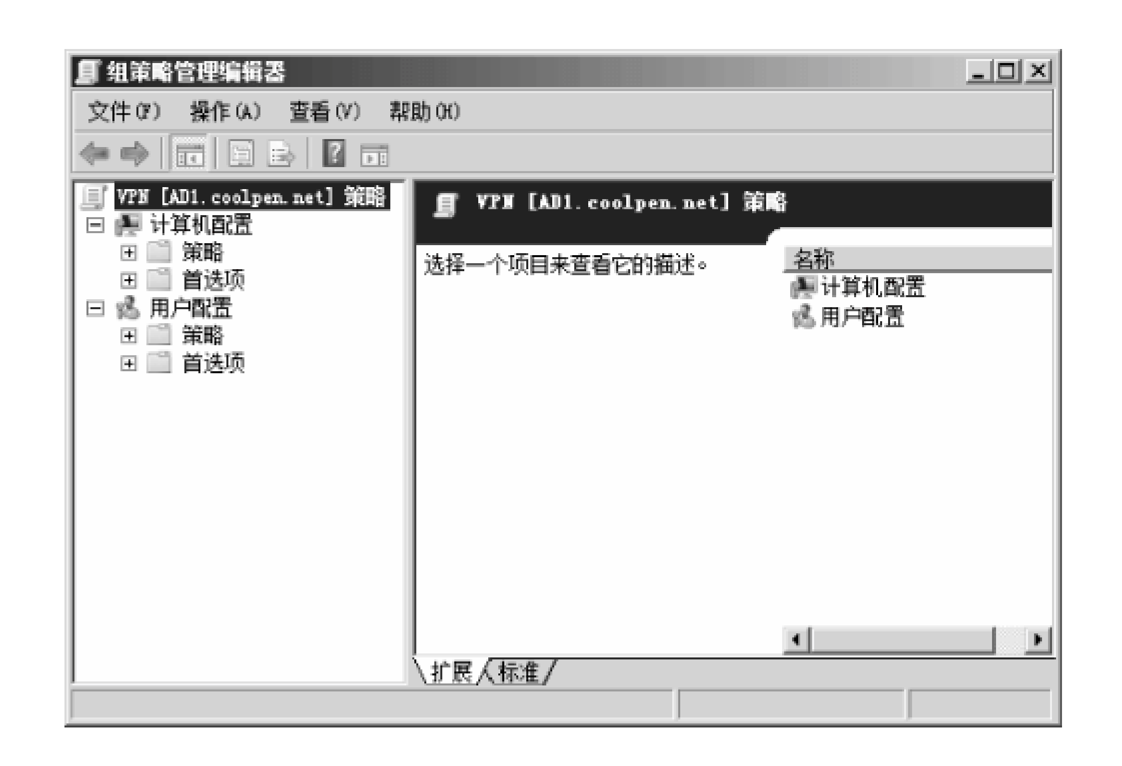


图 11-111　“新建 GPO”对话框　　　　图 11-112　“组策略管理编辑器”窗口



图 11-113　“启用安全中心(仅限域 PC) 属性”对话框

(3) 配置 NAP 客户端

在“组策略管理编辑器”窗口中,依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“网络访问保护”→“NAP 客户端配置”→“强制客户端”选项。在“强制客户端”窗口中,选择“远程访问隔离强制客户端”选项,右击并选择快捷菜单中的“属性”选项,打开“远程访问隔离强制客户端 属性”对话框。选中“启用此强制客户端”复选框,如图 11-114 所示。最后,单击“确定”按钮保存即可。

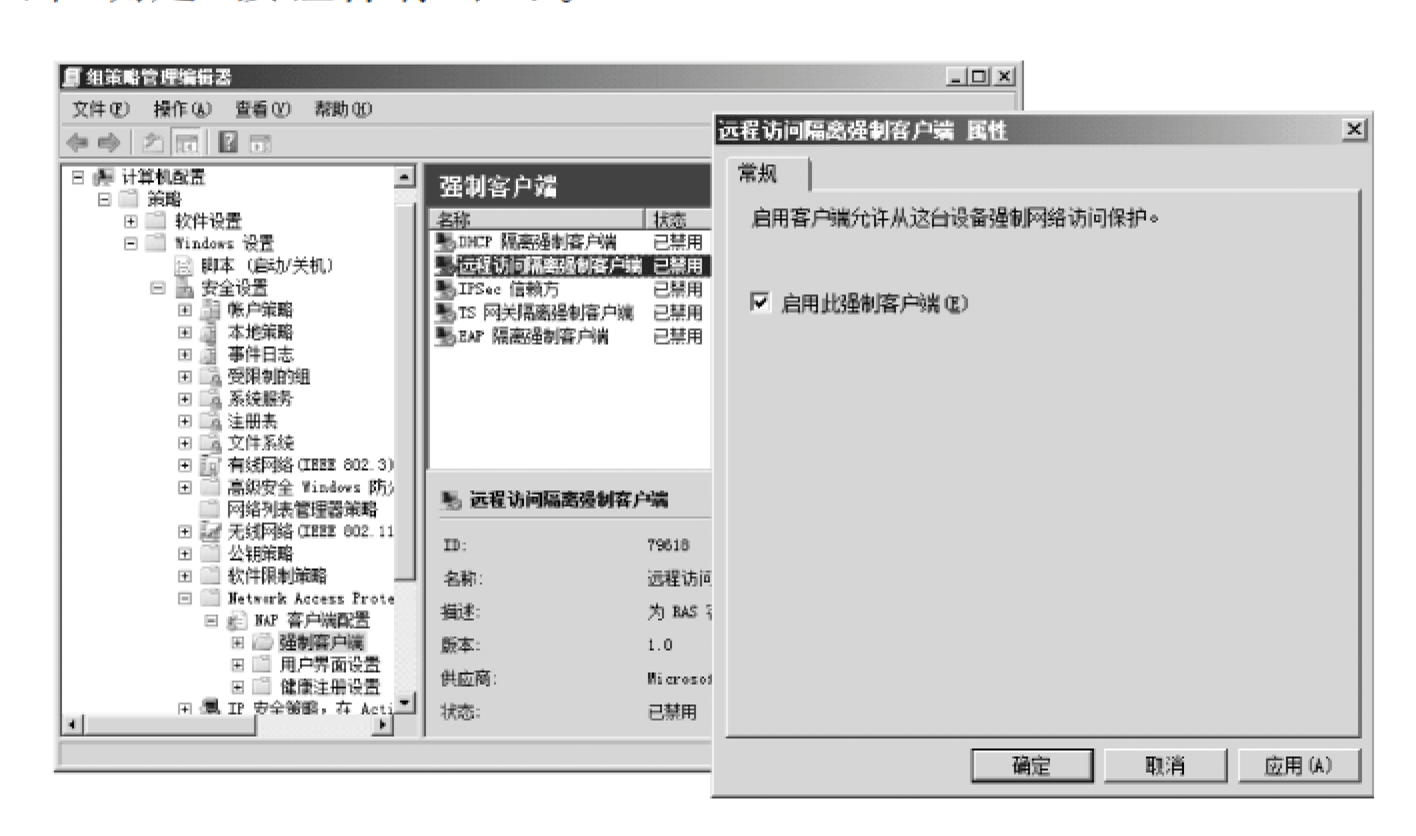


图 11-114 “远程访问隔离强制客户端 属性”对话框

(4) 配置 NAP 代理服务

在“组策略管理编辑器”窗口中,依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“系统服务”选项。选择 Network Access Protection Agent 选项,右击并选择快捷菜单中的“属性”选项,显示“Network Access Protection Agent 属性”对话框。选中“定义这个策略设置”复选框,并选中“自动”单选按钮,如图 11-115 所示。最后,单击“确定”按钮保存即可。



图 11-115 “Network Access Protection Agent 属性”对话框

11.5.4 测试受限 VPN 客户端的访问

在启用强制模式之前,用户必须测试不符合的 NAP 客户端的受限访问,以确保其可以被提示未通过评估的原因,并且只能访问受限网络中的补救服务器。

（1）在“网络连接”窗口中，双击 VPN 连接，输入用户名和密码并单击“确定”按钮，即可尝试连接到 VPN 服务器。由于已经设置健康策略验证，所以 VPN 客户端必须先提供验证证书，如图 11-116 所示。

（2）单击“确定”按钮，尝试链接到 VPN 服务器。此时，由于防火墙设置不符合健康策略要求，任务栏中显示“此计算机不符合该网络的要求”信息，如图 11-117 所示。



图 11-116　“验证服务器证书”对话框



图 11-117　此计算机不符合该网络的要求

（3）单击信息提示框，显示如图 11-118 所示的“网络访问保护”对话框。当前验证结果为“未成功”，修正结果为“管理员必须启用与 Windows 安全中心兼容的防火墙程序”。

（4）根据提示信息，启用 Windows 防火墙后，任务栏中将自动显示如图 11-119 所示的提示信息“此计算机符合该网络的要求”。



图 11-118　“网络访问保护”对话框(1)



图 11-119　此计算机符合该网络的要求

（5）此时单击信息框，显示如图 11-120 所示的“网络访问保护”对话框，即完全符合健康策略的要求。

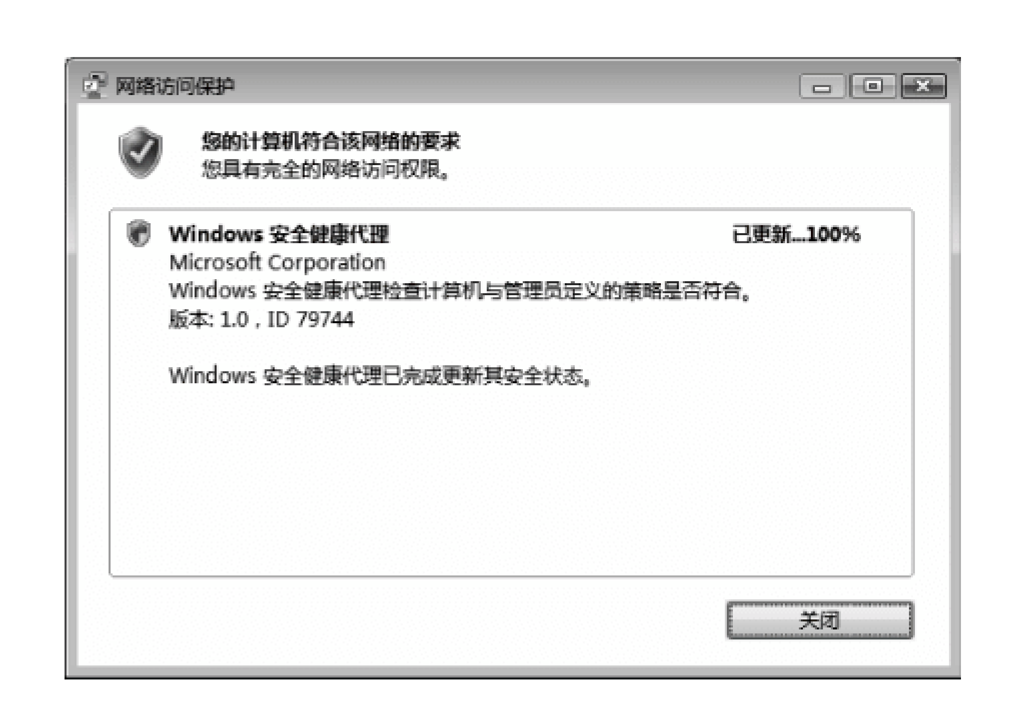


图 11-120 “网络访问保护”对话框(2)

11.6 配置 DHCP 强制

NAP DHCP 强制的目的是在 DHCP 客户端租借或续订其 IP 地址时，执行客户端健康检查，根据评估结果为其分配相应作用域的 IP 地址。通常情况下，需完成下列配置。

(1) 在 NPS 中，配置连接请求策略、网络策略和 NAP 健康策略。可以使用 NPS 控制台单独配置这些策略，也可以使用新建网络访问保护向导。

(2) 在可用 NAP 的客户端计算机上启用 DHCP 强制客户端和 NAP 服务。

(3) 在 DHCP 控制台中，为各个作用域或在 DHCP 服务器上配置的所有作用域启用 NAP。

(4) 配置网络策略服务器上的 SHV。

(5) 配置更新服务器组。

11.6.1 配置 NAP 健康策略服务器

与配置其他强制类型的 NPS 服务器相同，首先必须安装 NPS 服务器角色，然后安装和配置 SHV。由于 NAP DHCP 强制使用的是 NPS 服务器集成的 Windows 安全健康验证程序(WSHV)，所以无须安装 SHV。

1. 配置 RADIUS 服务器设置

由于 DHCP 服务器在配置 DHCP 强制之前，不需要使用 RADIUS 验证即可分配 IPv4 地址，所以 NAP 健康策略服务器通常没有将 DHCP 服务器配置为 RADIUS 客户端。用户必须通过 NPS 管理单元添加 DHCP 服务器到 NAP 健康策略服务器上。当在“新建 RADIUS 客户端”对话框中，配置 RADIUS 客户端时，必须选中“RADIUS 客户端启用 NAP”复选框。

此外由于 DHCP 强制配置将使用报告模式，不符合的 NAP 客户端拥有不受限的访问，所以用户在启用强制模式之前可能需要更改 NAP 健康策略服务器的登录入站请求。用户可以配置 NPS 服务记录入站请求和记账信息在本地 SQL 服务器数据库文件中。

2. 为 DHCP 强制配置健康要求策略

用户可以手动或者通过“配置 NAP 向导”为 DHCP 强制创建健康要求策略。由于通过“配置 NAP 向导”进行的配置为自动完成的，所以推荐使用这种方法。

（1）打开“网络策略管理器”窗口，单击 NPS，在“标准配置”下拉列表框中选择“网络访问保护(NAP)”。单击“配置 NAP”链接，显示如图 11-121 所示的“选择与 NAP 一起使用的网络连接方法”对话框，在“网络连接方法”中，选择“动态主机配置协议(DHCP)”，在“策略名称”文本框中，默认名称为 NAP DHCP，用户也可以自定义。

（2）单击“下一步”按钮，显示如图 11-122 所示的“指定 NAP 强制服务器运行 DHCP 服务器”对话框。单击“添加”按钮，即可添加符合启用 NAP 的 DHCP 服务器的 RADIUS 客户端。



图 11-121 “选择与 NAP 一起使用的网络连接方法”对话框



图 11-122 “指定 NAP 强制服务器运行 DHCP 服务器”对话框

（3）单击“下一步”按钮，显示如图 11-123 所示的“指定 DHCP 作用域”对话框，单击“添加”按钮，为健康要求策略添加标识 DHCP 作用域的配置文件名称。如果创建任何名称，则对 DHCP 服务器上的所有作用域启用 DHCP 强制。

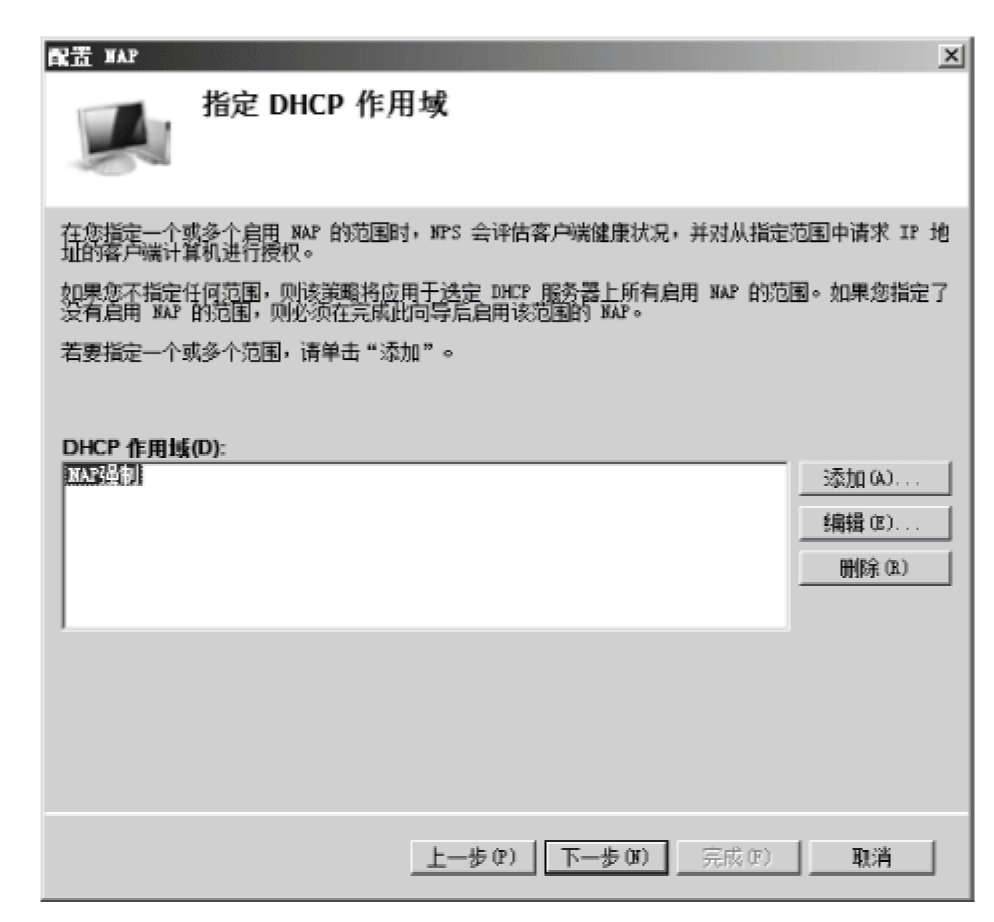


图 11-123 “指定 DHCP 作用域”对话框

（4）单击“下一步”按钮，显示“配置用户组和计算机组”对话框，根据需要选择计算机或组。单击“下一步”按钮，指定 NAP 更新服务器组和 URL，选择希望应用的更新服务器组即可，此处不再赘述。

（5）单击“下一步”按钮，显示“定义 NAP 健康策略”对话框，选择 DHCP 强制需要评估的 SHV。选择“启用客户端计算机的自动更新”选项，并选中“允许对不具有 NAP 功能的客户端计算机的完全网络访问权限”单选按钮，即使用户想要不支持 NAP 功能的客户端拥有受限访问。因为用户想要最初的 NAP 强制模式为报告模式，所以用户必须选择“允许对不具有 NAP 功能的客户端计算机的完全网络访问权限”。在配置强制模式的过程中，用户可以为不具有 NAP 功能的客户端更改网络策略来限制访问。

(6) 单击“下一步”按钮，显示“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框，提示由该向导创建的各种策略以及 RADIUS 客户端和更新服务器组。

(7) 单击“完成”按钮，关闭“配置 NAP”向导即可。

“配置 NAP 向导”创建的连接请求策略和网络策略位于各自顺序列表的底部。由于不符合的 NAP 客户端网络策略默认情况下只允许受限访问(强制模式)，用户必须修改该策略使之允许报告模式下的不受限访问。

3. 为系统健康要求配置评估条件

(1) 打开“网络策略服务器”窗口，依次展开“策略”→“健康策略”选项，如图 11-124 所示。显示了通过配置 NAP 向导创建的健康策略，包括“NAP DHCP 符合”和“NAP DHCP 不符合”两条。

(2) 双击“NAP DHCP 不符合”健康策略，显示如图 11-125 所示的“NAP DHCP 不符合 属性”对话框。根据实际需要，在“客户端 SHV 检查”下拉列表框中选择相应级别的标准，如“客户端未能通过所有 SHV 检查”等。“NAP DHCP 符合”健康策略的条件设置，与之完全相同，此处不再赘述。

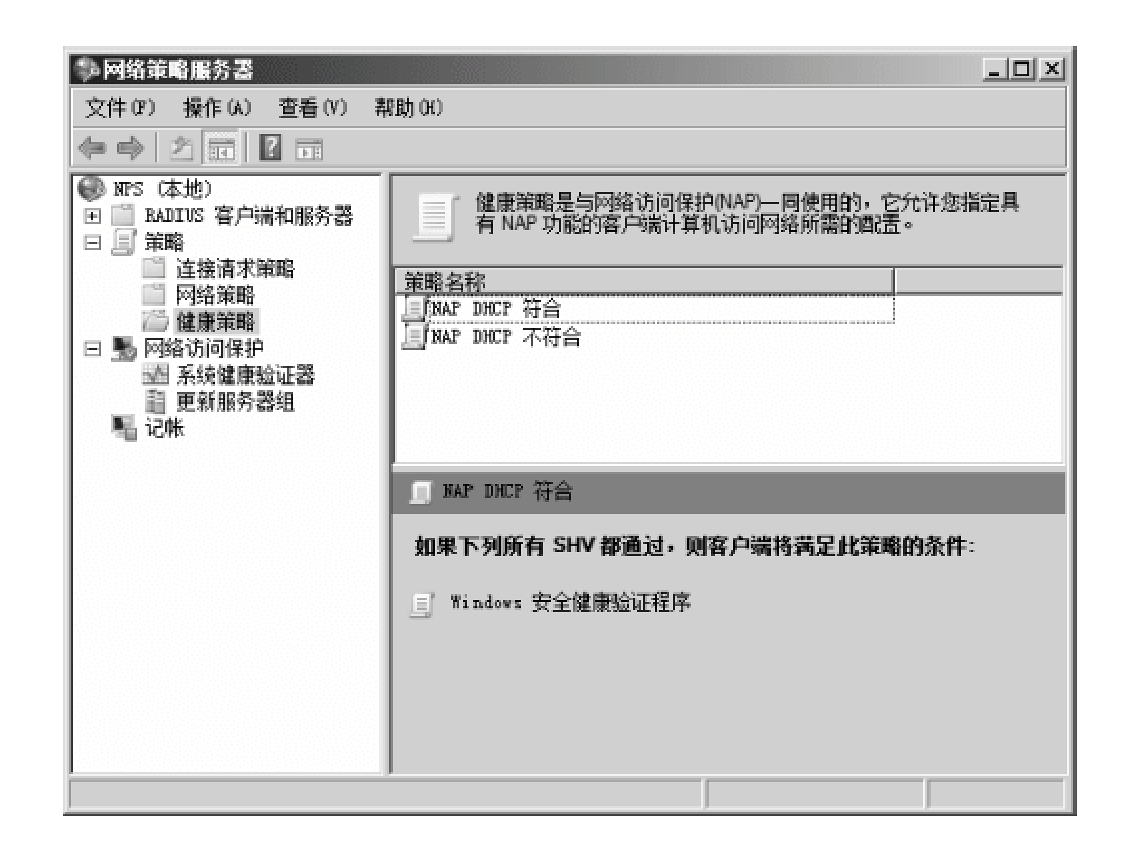



图 11-124 “网络策略服务器”窗口

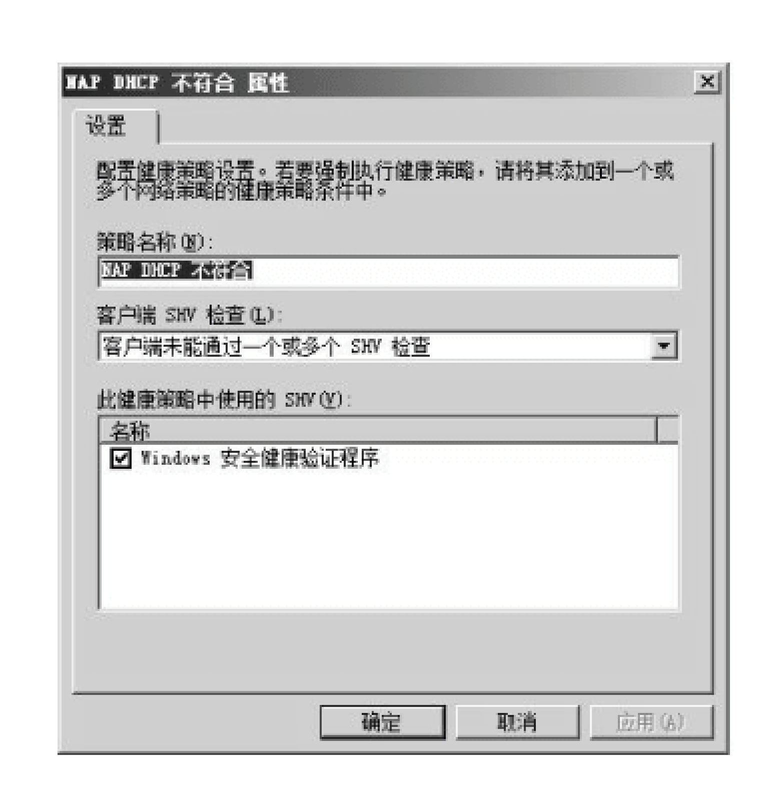


图 11-125 “NAP DHCP 不符合 属性”对话框

4. 允许免除安全组完全访问

在准备工作中，已经在域中创建了免除安全组，并将需要免除的计算机添加到组中。在网络策略服务器上，必须为这些计算机创建单独的网络访问策略，使其免除 DHCP 强制。

(1) 打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”选项。右击“配置 NAP 向导”为符合的 NAP 客户端创建的 DHCP 网络策略，在快捷菜单中选择“重复策略”选项，可以看到副本，默认是禁用的，如图 11-126 所示。

(2) 双击“副本 NAP DHCP 符合”策略，显示如图 11-127 所示的“副本 NAP DHCP 符合 属性”对话框。在“概述”选项卡中，可以重新定义策略名称，例如“DHCP 免除安全组”。在“策略状态”区域，选中“策略已启用”复选框，并选中“授予访问权限”单选按钮。

(3) 切换至“条件”选项卡，单击“添加”按钮，显示“选择条件”对话框，选中“Windows 组”并单击“添加”按钮，显示“Windows 组”对话框，将创建好的免除安全组添加进来即可，如图 11-128 所示。

(4) 连续单击“确定”按钮，保存设置。同时在“条件”选项卡中删除除默认“健康策略”



图 11-126 “网络策略服务器”窗口

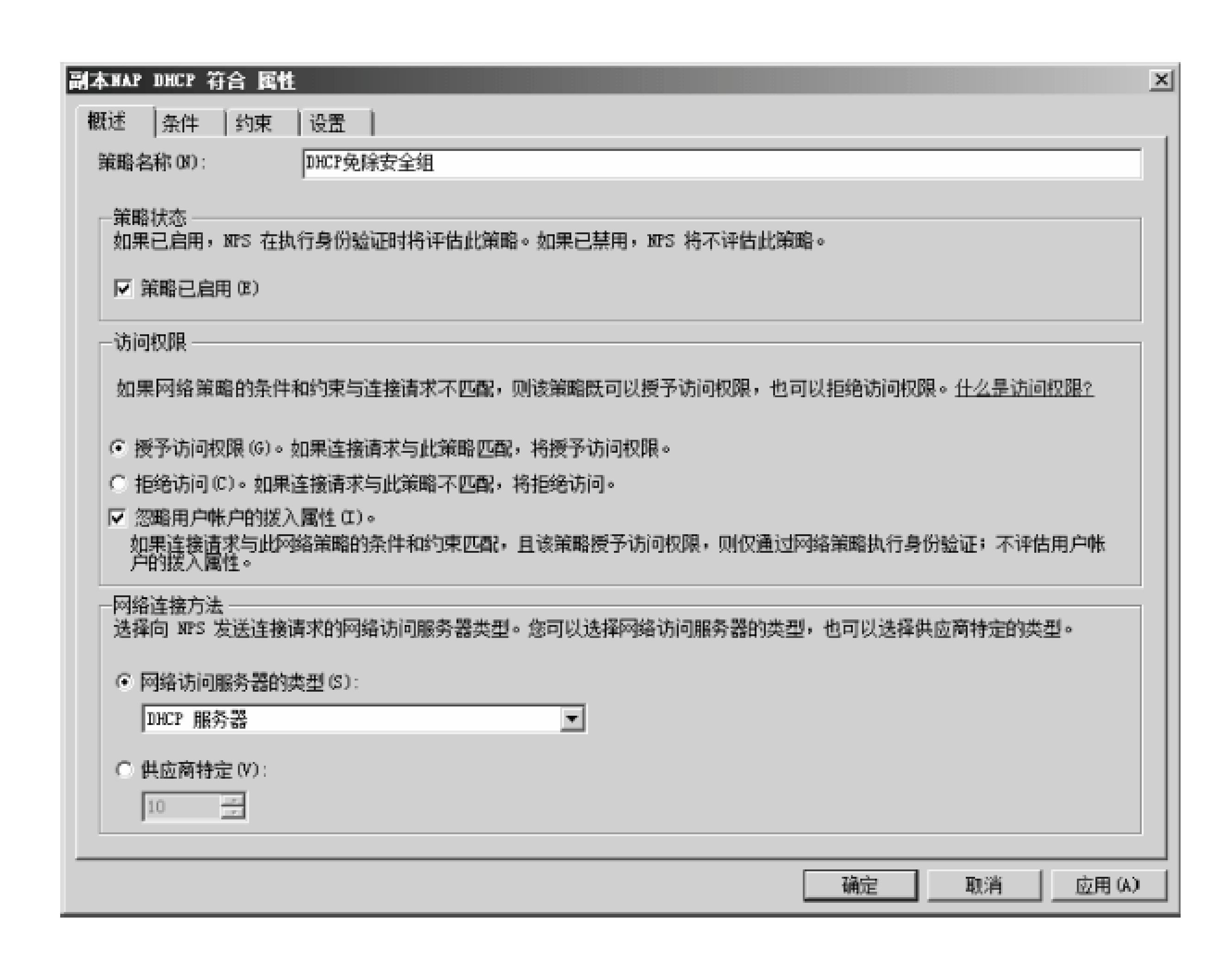


图 11-127 “概述”选项卡



图 11-128 “条件”选项卡

之外的所有条件。

(5) 在“网络策略”窗口中,将用于免除安全组的健康策略移动到最前端,以确保对所有客户端先实施此策略评估。

11.6.2 配置 NAP 客户端

同其他类型的 NAP 客户端类似,管理员可以通过多种方式配置 NAP 客户端。如果客户端是域成员计算机,则可以借助组策略统一部署。如果是独立计算机,则可以通过修改客户端计算机的本地策略完成。主要配置操作如下。

(1) 配置 NAP 客户端设置。

(2) 启用 Windows 安全中心(参考“配置 VPN 强制”中 NAP 客户端的配置)。

(3) 配置网络访问保护代理服务的自动启用(参考“配置 VPN 强制”中 NAP 客户端的配置)。

注意: DHCP NAP 强制客户端中需要配置的“DHCP 隔离强制客户端”,系统默认是禁用,用户只需借助组策略或其他手段,启用该功能即可,如图 11-129 所示。NAP 客户端的其他配置与 VPN 强制客户端完全相同,此处不再赘述。



图 11-129 配置 NAP 客户端

11.6.3 将 DHCP 服务器配置为 RADIUS 客户端

NPS 服务器之所以能够响应客户端的 DHCP 请求,评估系统健康程度,就是基于 NPS 服务器的 RADIUS 服务器,在中间起了至关重要的转发作用。因此,必须先将 DHCP 服务器配置为 RADIUS 服务器的客户端。

(1) 打开“网络策略服务器”窗口,依次展开“RADIUS 客户端和服务器”→“RADIUS 客户端”选项,显示如图 11-130 所示的窗口。由于在配置 NPS 服务器的网络策略时,已经将 DHCP 服务器设置为 RADIUS 客户端,不过此时并不支持 NAP。

(2) 右击 RADIUS 客户端,选择“属性”选项,显示如图 11-131 所示的“DHCP 属性”对话框。选中“启用此 RADIUS 客户端”和“RADIUS 客户端支持 NAP”复选框。其他选项保持默认设置即可。




图 11-130　“网络策略服务器”窗口

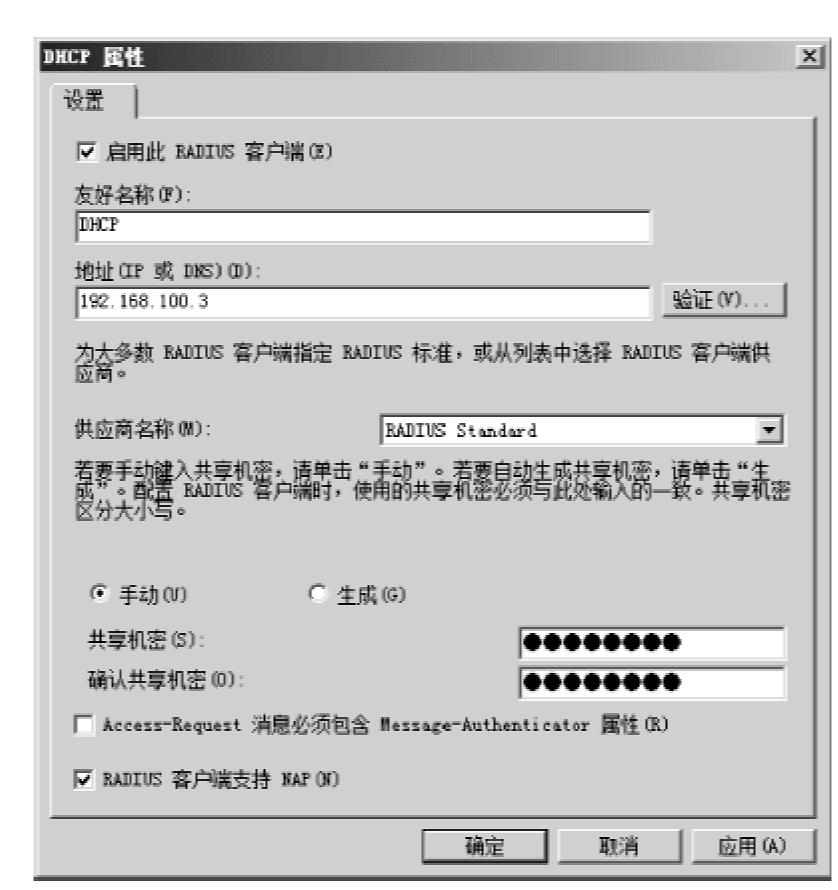


图 11-131　“DHCP 属性”对话框

11.6.4　配置 DHCP 服务器选项

当 DHCP 服务器被配置为 NPS 服务器，或者所在网络中新增 NPS 服务器后，原有 DHCP 服务将被新的包含 NPS 功能的组件所取代，管理员需要对 NPS 涉及的 DHCP 选项进行重新配置。默认状态下，NPS 关联的组件没有启用。

1. 配置作用域

NPS 安装完成后，在 DHCP 作用域属性中，添加了一项“网络访问保护”选项卡，默认情况下，该设置没有启用，需要网络管理员启用该设置。

在 DHCP 控制台窗口中，依次展开“AD2. coolpen. net（服务器名称）”→IPv4 选项，显示当前 DHCP 上的所有作用域。首先，右击想要配置网络安全防护的作用域并选择“属性”选项，打开“作用域 属性”对话框，然后切换至“网络访问保护”选项卡。在“网络访问保护设置”选项区中，选中“对此作用域启用”单选按钮，如图 11-132 所示。如果在 NPS 服务器上设置了标识作用域配置文件的名称，则可以选中“使用自定义配置文件”单选按钮，并在“配置文件名”文本框中，输入指定的名称。

注意：如果此服务器同时提供 IPv6 下的 DHCP 服务，则还需要在 IPv6 的所有作用域中，执行相同操作。

2. 配置服务器选项

NAP 通过新的 NAP“用户类作用域”选项，使计算机在同一作用域内的受限网络和不受限网络访问之间切换。在为状态不良的客户端计算机提供租约时，会使用这组特殊的作用域选项（DNS 服务器、DNS 域名、路由器等）。例如，提供给状态良好的客户端的默认 DNS 后缀为 coolpen. net，而状态不良的客户端提供的 DNS 后缀为 unsafecoolpen. net。

（1）在 DHCP 管理窗口中，依次展开 DHCP→“lxh-2008. coolpen. net（服务器名）”→IPv4→“服务器选项”选项，右击“服务器选项”并选择快捷菜单中的“配置选项”选项，显示如图 11-133 所示的“服务器 选项”对话框。

（2）切换至“高级”选项卡，在“供应商类别”下拉列表框中，选择“DHCP 标准选项”选项；在“用户类别”下拉列表框中，选择“默认的网络访问保护级别”选项，如图 11-134 所示。

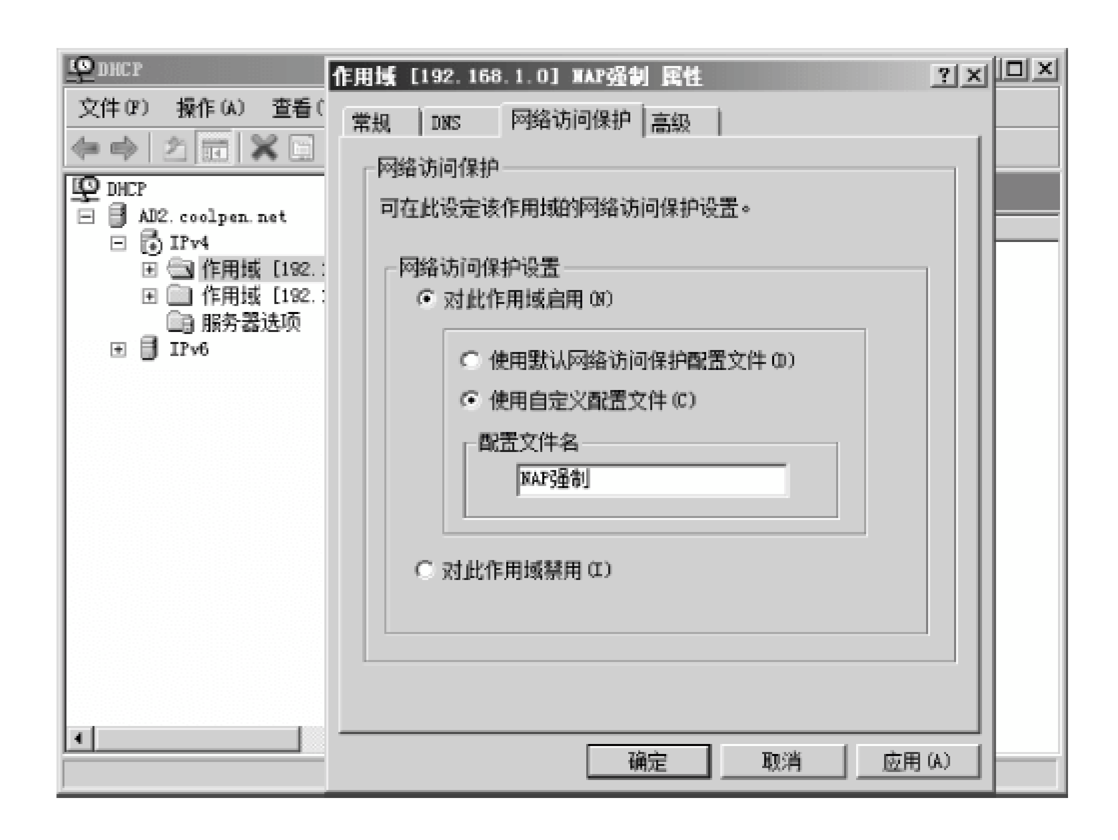


图 11-132　配置 DHCP 作用域



图 11-133　“服务器 选项”对话框



图 11-134　“高级”选项卡

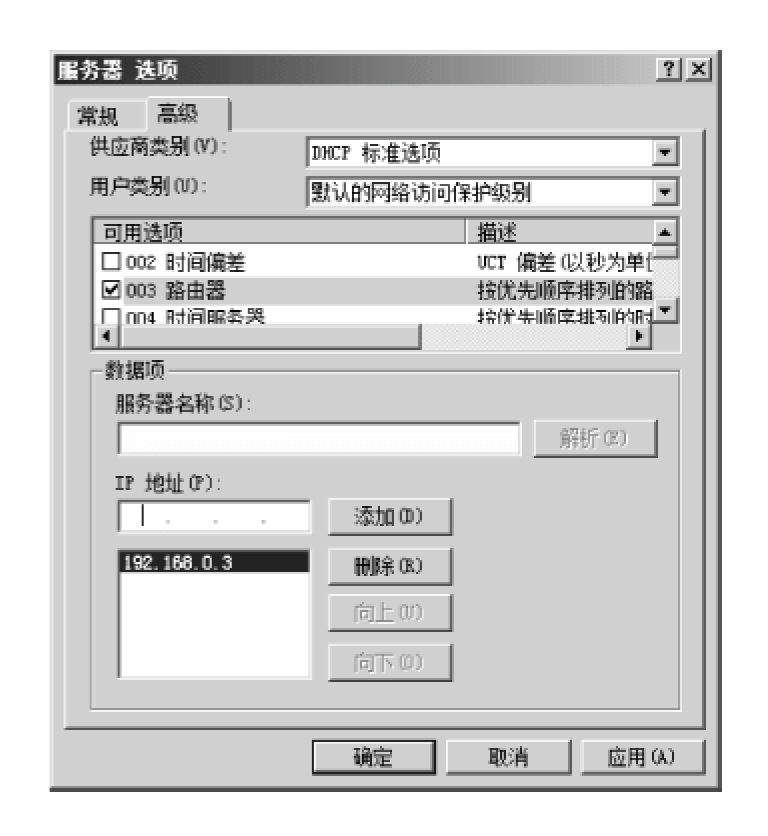


图 11-135　003 路由器

(3) 在“可用选项”列表中，选中“003 路由器”复选框，在“IP 地址”文本框中，输入网络中路由器使用的 IP 地址，例如 192.168.0.3，单击“添加”按钮。如果网络中有多个路由器，可以再次添加。如果发现路由器的顺序错误，则可以单击“下移”按钮或者“上移”按钮，调整路由器的顺序，如图 11-135 所示。

(4) 在“可用选项”列表中，选中“006 DNS 服务器”复选框，在“IP 地址”文本框中，输入网络中 DNS 服务器使用的 IP 地址，单击“添加”按钮。如果网络中有多个 DNS，可以逐次添加。如果发现 DNS 服务器的顺序错误，则可以单击“下移”按钮或者“上移”按钮，调整 DNS 服务器的顺序，如图 11-136 所示。

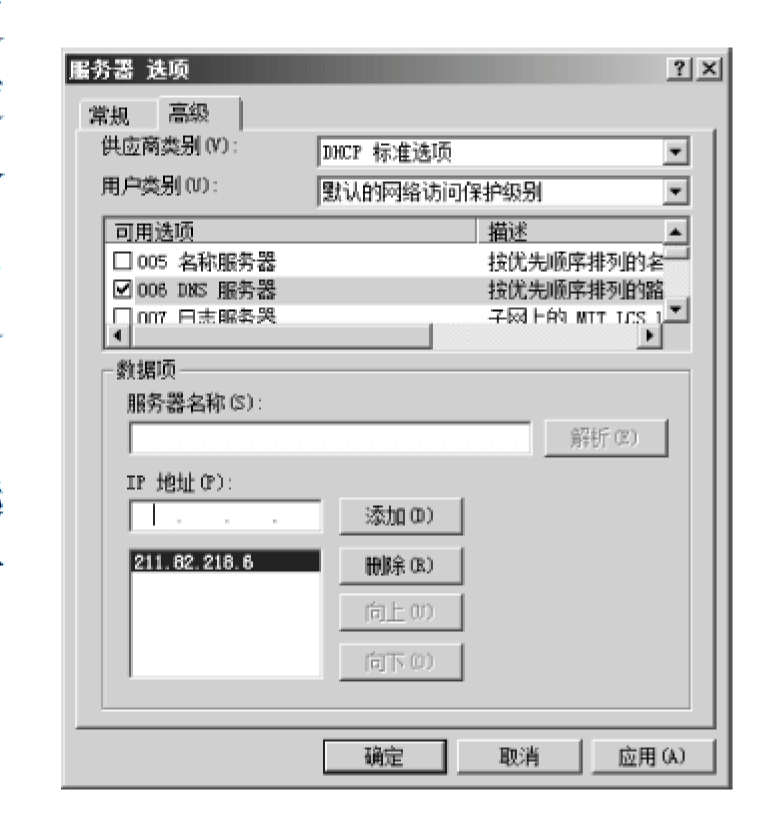


图 11-136　006 DNS 服务器

(5) 在“可用选项”列表中，选中“015 DNS 域名”复选框，在“数据项”选项区的“字符串值”文本框中，输入临时的 DNS 域名，如图 11-137 所示。

提示：临时域的域名和 DHCP 安装过程创建的域名不同，没有实际的作用，只是方便网络管理员区分连到网络中的计算机，哪些是安全的，哪些是不安全的。例如，如

果计算机是安全的，则使用 coolpen. net 域名；如果计算机不是安全的，则使用这里指定的 unsafecoolpen. net 域名。

(6) 单击“确定”按钮，完成服务器选项的设置，如图 11-138 所示。




图 11-137　015 DNS 域名



图 11-138　配置完成后的作用域选项

11.6.5　测试 DHCP 强制客户端

测试 DHCP 强制配置结果是否成功，只需在指定客户端上修改其安全配置，使其符合健康策略和不符合安全健康策略，然后查看其获取的 IP 地址类型即可。

如果客户端在关闭系统防火墙或者没有安装最新更新补丁的情况下，登录域控制器，或者登录域后关闭了某些 Windows 安全功能，则此时任务栏中会提示如图 11-139 所示的“此计算机不符合该网络的要求”信息。证明 NAP 服务器开始发挥作用。

此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 11-140 所示的“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解决问题的方案。这些提示方法就是系统健康策略模板中管理员设定的处理操作。

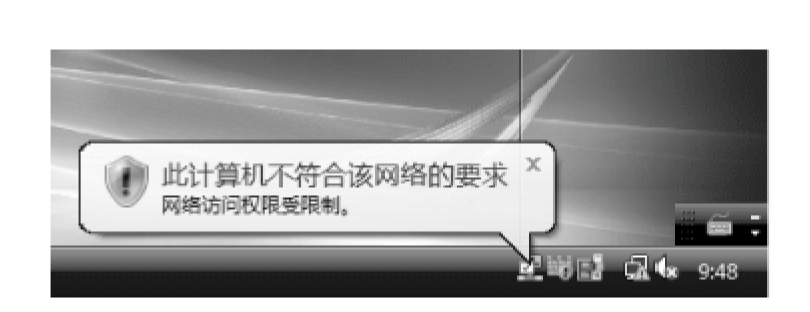


图 11-139　此计算机不符合该网络的要求

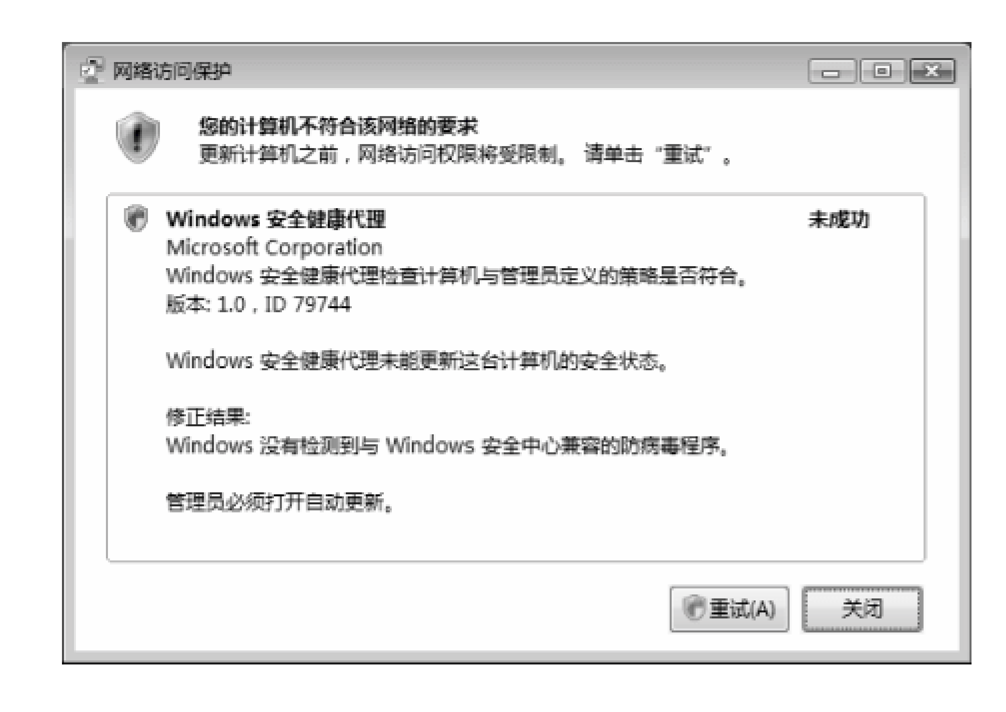


图 11-140　“网络访问保护”对话框(3)

打开命令提示符窗口，输入 ipconfig/renew 命令，重新获取 IP 地址，再使用 ipconfig 命令，查看当前 IP 地址，显示如图 11-141 所示结果。在 DHCP 服务器上为不安全客户端分配的 IP 地址是 192.168.2.10～192.168.2.100，而此次测试中获取的 IP 地址是 192.168.2.11，恰恰是该范围内的地址。



图 11-141 作为不安全客户端时获取的 IP 地址

用户可以根据提示信息尝试解决相关问题，如开启系统防火墙、恶意软件保护功能或将系统升级到最新等。处理完毕后，任务栏中会出现如图 11-142 所示的提示信息。

此时，单击“此计算机符合该网络的要求”提示信息，会显示如图 11-143 所示的“网络访问保护”对话框，提示已具有完全的网络访问权限。

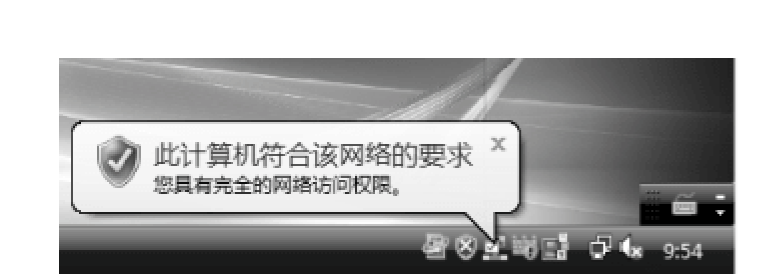


图 11-142 此计算机符合该网络的要求

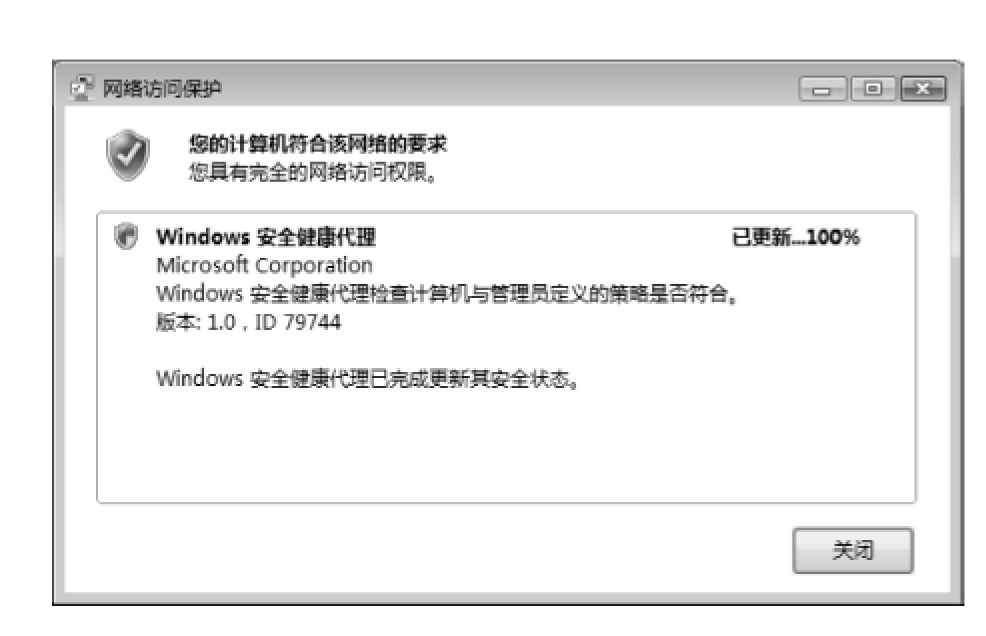


图 11-143 “网络访问保护”对话框(4)

再次重新获取 IP 地址，并使用 ipconfig 命令查看，显示如图 11-144 所示结果。此次获取的 IP 地址是 192.168.1.101，与 DHCP 服务器上指定的 192.168.1.100～192.168.1.200 相符，说明 DHCP 强制配置成功。



图 11-144 作为安全客户端时获取的 IP 地址

习题

1. 简述 NAP 的运行机制。
2. NAP 技术的主要应用领域有哪些?
3. 简述 NAP 系统的基本组成。
4. 部署 NAP 客户端的方式有哪些?

实验:配置 TS 网关强制

实验目的:

掌握 NAP 强制的基本应用。

实验内容:

在企业网络中配置 TS 网关,并通过 NAP 强制系统对使用 TS 服务器实现远程管理的客户端进行系统健康评估。

实验步骤:

(1) 配置 NAP 系统。

(2) 配置 TS 服务器。

(3) 在 NAP 服务器上创建对远程 TS 连接的强制策略。

(4) 在客户端计算机上尝试通过 TS 服务器访问服务器远程桌面,验证 NAP 强制是否有效。

第 12 章 chapter 12

安全设备规划与配置

随着计算机网络应用领域的不断延伸,信息安全已经成为关乎每个用户的问题。一个企业网络中可以没有服务器,但绝不能没有安全保障系统。局域网中常见的安全设备包括网络防火墙、入侵检测系统、入侵防御系统等,这些设备分布在网络中的不同位置,可以为整个网络或重点对象提供更可靠的保护。

12.1 网络安全设备规划

本案例涉及的计算机网络是一个拥有 500 个信息点、百兆接入 Internet 的中型企业网络。公司内部大部分业务也转向网络平台,在充分享受计算机网络带来的快速、灵活、便利的同时,也随时面临着网络安全带来的不利影响。因此,在原有网络基础上实施一套完整、可操作的安全解决方案不仅是可行的,而且是必需的。

12.1.1 案例情景

企业通过 Internet 可以把遍布世界各地的资源拿来共享,也可以为自身树立良好的企业形象。由于 Internet 的高度开放性,企业网络接入 Internet 无疑会面临更多的风险。这也是该企业网络一直没有全面接入 Internet 的主要原因。目前,企业网络中的部分服务器只对内网提供服务,并未连接到 Internet。随着企业不断将更多的商务活动转移到网络,针对网络系统的非法入侵、病毒活动也随之增多。现有的被动安全防御体系越来越显得微不足道。

目前,现有的网络安全防御措施都是基于网络服务器、路由器和交换机的,通常以被动防御为主。服务器感染病毒可以通过网络防病毒系统扫描和查杀病毒;通过用户账户权限分配,使普通用户无法访问网络中的机密数据信息。另外,内部网络按照所属的部门、职能、安全重要程度分为许多子网,例如办公区内划分了财务部、人事部、领导部门等,并且在核心交换机上为不同的逻辑子网划分了不同的 VLAN,严格避免来自内部网络的隐患。

目前,该企业局域网存在以下安全隐患。

(1) 网络与 Internet 直接连接,可能通过 Internet 访问造成病毒、黑客攻击以及来自 Internet 的非法授权访问等。

(2) 网络中的部分应用服务器需要将服务发布到 Internet,可能造成公开服务器的安全风险扩散到内部。

(3) 内部网络中存在许多不同的子网,不同的子网有不同的安全性,需要将不同功能和

安全级别的网络加以区分。

12.1.2 项目需求

企业网络的信息完全防御系统不应该仅仅是建立在信息理论与技术手段上,也不能仅仅依靠安全的通信协议和严格的访问控制策略。网络安全设备的重要作用也是不容忽视的。安全分析技术的源数据主要来自安全设备,只有硬件设备与现有技术手段相辅相成,才能充分发挥各自的安全防护功能。

在该企业网络中,安全问题主要集中在服务器防护上,包括防病毒、防黑客入侵等,另外还包括内部网络重要子网的安全防护,如财务部子网、领导部门等。目前,网络安全项目的总体需求如下。

(1) 公开服务器的安全保护。

(2) 防止黑客从外部攻击。

(3) 入侵检测与监控。

(4) 信息审计与记录。

(5) 病毒防护。

(6) 数据安全保护。

(7) 数据备份与恢复。

(8) 互联网访问安全管理。

在部署安全系统时,应该满足以下需求。

(1) 大幅度地提高系统的安全性(重点是可用性、可控性和主动防御)。

(2) 保持网络原有特点,对网络协议和传输具有很好的透明性,能透明接入,无须更改网络设置。

(3) 易于操作、维护并便于管理,不增加或少增加附加操作。

(4) 尽量不影响原网络拓扑结构,同时便于系统及系统功能的扩展。

(5) 安全保密系统具有较好的性价比,一次性投资,长期使用。

(6) 安全产品具有合法性,已经过国家有关管理部门的认可或认证。

12.1.3 解决方案

网络安全解决方案的优劣直接关系到企业信息网络的安全性。网络的安全性并不是取决于使用了哪些安全新技术,部署了哪些安全设备,更重要的是这些技术和设备运用是否合理、得当。针对该企业的网络安全现状,将通过在网络中部署网络防火墙、入侵检测系统和入侵防御系统,解决用户的安全需求问题。

1. 网关安全——网络防火墙

网关是指局域网的出口,即局域网连接到 Internet 接口。通常在网关处部署防火墙。传统的硬件防火墙支持协议层过滤,阻断未经允许的端口访问。应用层防火墙可以对应用层的数据包进行过滤,拒绝可疑的数据包。Cisco 公司的 ASA 系列产品,完成协议层过滤,利用访问控制列表过滤目标站点。图 12-1 所示是本方案中采用的 Cisco ASA 5500 系列防火墙。Cisco ASA 5500 系列自适应安全设备是一个模块化平台,为中小型企业应用提供了全面的安全服务,包括防火墙、入侵防御系统、Anti-X 和 VPN 服务等。

2. 局部安全——IDS

对于企业网络中安全要求较高且容易受到攻击的对象可以实施重点保护，例如办公子网、服务器子网等。IDS(Intrusion Detection Systems，入侵检测系统)作为一种网络安全的监测设备，可以依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。图 12-2 所示是本解决方案中使用的 Cisco IDS 4250。



图 12-1 Cisco ASA 5500 防火墙



图 12-2 Cisco IDS 4250

通过在服务器区域的汇聚交换机上部署 IDS，可以确保网络服务器的安全。IDS 在捕捉到某一攻击事件后，按策略进行检查，如果策略中对该攻击事件设置了防火墙阻断，那么，入侵检测系统就会发给防火墙一个相应的动态阻断策略，防火墙根据该动态策略中的设置进行相应的阻断，阻断的时间、阻断时间间隔、源端口、目的端口、源 IP 和目的 IP 等信息，完全依照入侵检测系统发出的动态策略来执行。总的来说，联动有一定效果，但是稳定性不理想。

3. 全网安全防护——IPS

部署在网关处的网络防火墙已经可以起到整个网络安全的作用，但由于其工作原理简单，仅能对已经存在的安全威胁因素进行拦截和过滤。而通过在网络防火墙的后面再部署 IPS (Intrusion Prevention System，入侵防御系统)，不仅可以实时捕获和分析网络数据流，发现潜在的网络攻击因素，而且可以实时多种相应方式。图 12-3 所示为 Cisco IPS 4260 入侵防御设备。



图 12-3 Cisco IPS 4260 入侵防御设备

12.2 网络安全设计

网络安全设备种类繁多，而且产品质量良莠不齐，例如 Cisco 公司的安全设备就包括 Cisco PIX、Cisco ASA、Cisco FWSM、Cisco IDS、Cisco IPS、Cisco VPN 等，并且随着产品整合程度的不断提升，大部分辅助安全设备已经实现模块化，大大节约了用户组网成本，便于集中控制和管理。不过需要注意的是，不同的安全设备在网络中的位置是有所不同的，选择安全设备时不仅要注意产品类型、厂家，更应结合自己的实际需要。

12.2.1 网络防火墙设计

网络防火墙的主要特点是只能对通过它的数据包进行拦截和过滤，通常需要部署在被保护网络的边界，如局域网接入 Internet 时，就应将防火墙部署在局域网的出口处。网络防火墙可以应用于以下 4 种网络环境。

1. 内部网络与 Internet 的连接之间

内部网络与 Internet 的连接之间是防火墙应用最广，也是最重要的应用环境。在这种

应用环境下，防火墙主要保护内部网络不遭受非法用户的攻击。这也是目前绝大多数企业网络安装防火墙的主要目的。一般可将防火墙网络划分为3个不同级别的安全区域，如表12-1和图12-4所示。

表12-1　连接内外网防火墙的不同安全区

安全区域	说　　明
内部网络	这是防火墙要保护的对象，包括全部的企业内部网络设备及用户主机，这个区域是防火墙的可信区域(这是由传统防火墙的设计理念决定的)
外部网络	这是防火墙要防护的对象，包括Internet主机和设备，这个区域为防火墙的不可信网络区域(也是由传统防火墙的设计理念决定的)
非军事区(Demilitarized Zone，DMZ)	它是从企业内部网络中划分的一个小区域，其中包括内部网络中用于公众服务的外部服务器，如Web服务器、邮件服务器、FTP服务器和外部DNS服务器等，它们都是为Internet提供某种信息服务的

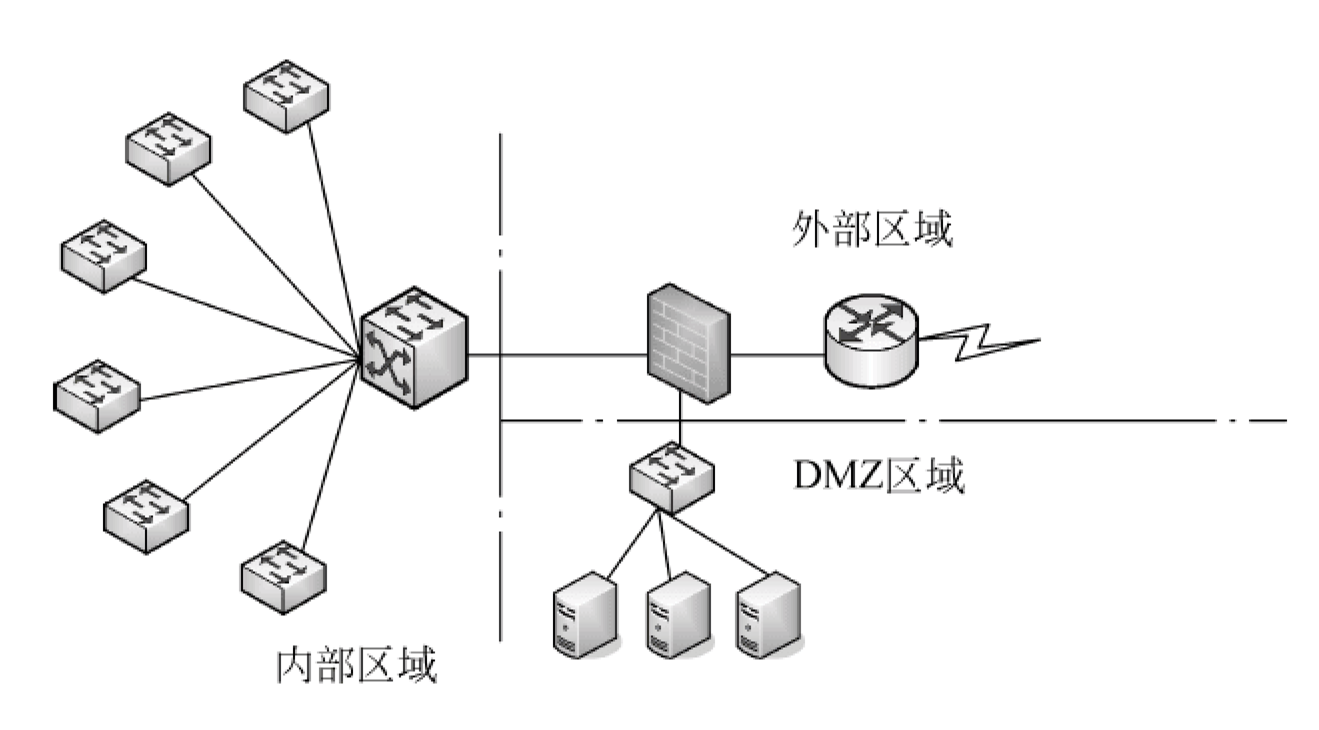


图12-4　防火墙分割的3个区域

在这3个区域中，用户需要对不同的安全区域给予不同的安全策略。虽然内部网络和DMZ区都属于企业内部网络的一部分，但它们的安全级别(策略)是不同的。对于要保护的大部分内部网络，一般情况下禁止所有来自Internet用户的访问。由企业内部网络划分出去的DMZ区，因要为Internet应用提供相关的服务，所以在一定程度上，没有内部网络限制那么严格，如Web服务器通常是允许任何人进行正常的访问。

这些服务器是不是很容易被攻击呢？由于在这些服务器上所安装的服务非常少，所允许的权限非常低，真正有服务器数据的是在受保护的内部网络主机上。所以，黑客攻击这些服务器没有任何意义，既不能获取什么有用的信息，也不能通过攻击它而获得过高的网络访问权限。

提示：建议通过NAT(网络地址转换)技术将受保护的内部网络的全部主机地址映射成防火墙上设置的少数几个有效公网IP地址。这样有两个好处：其一可以对外屏蔽内部网络和IP地址，保护内部网络的安全；其二由于公网IP地址共享，所以可以大大节省公网IP地址的使用，节省了企业投资成本。

2. 连接局域网和广域网

局域网和广域网之间的连接也是应用防火墙最多的地方，不过，网络用户根据自己具体需要的不同，有两种连接方式可供选择。

如果用户网络原来已存在边界路由器，则可充分利用原有设备，利用边界路由器的包过滤功能，添加相应的防火墙配置，这样原来的路由器也就具有防火墙功能了。然后再利用防火墙与需要保护的内部网络连接。

对于 DMZ 区中的公用服务器，可以直接与边界路由器相连，只经过路由器的简单防护，而不经过防火墙。边界路由器与防火墙就一起组成了两道安全防线，如图 12-5 所示，并且在这两者之间可以设置一个 DMZ 区，用来放置那些允许外部用户访问的公用服务器设施。

如果用户网络中不存在边界路由器，则此时直接由防火墙来保护内部网络，如图 12-6 所示。此时 DMZ 区域和需要保护的内部网络分别连接防火墙的不同 LAN 网络接口。因此，需要对这两部分网络设置不同的安全策略。这种网络中虽然只有一道安全防线，但对于大多数中小企业来说是完全可以满足的。不过在选购防火墙时就要注意，防火墙一定要有两个以上的 LAN 网络接口。

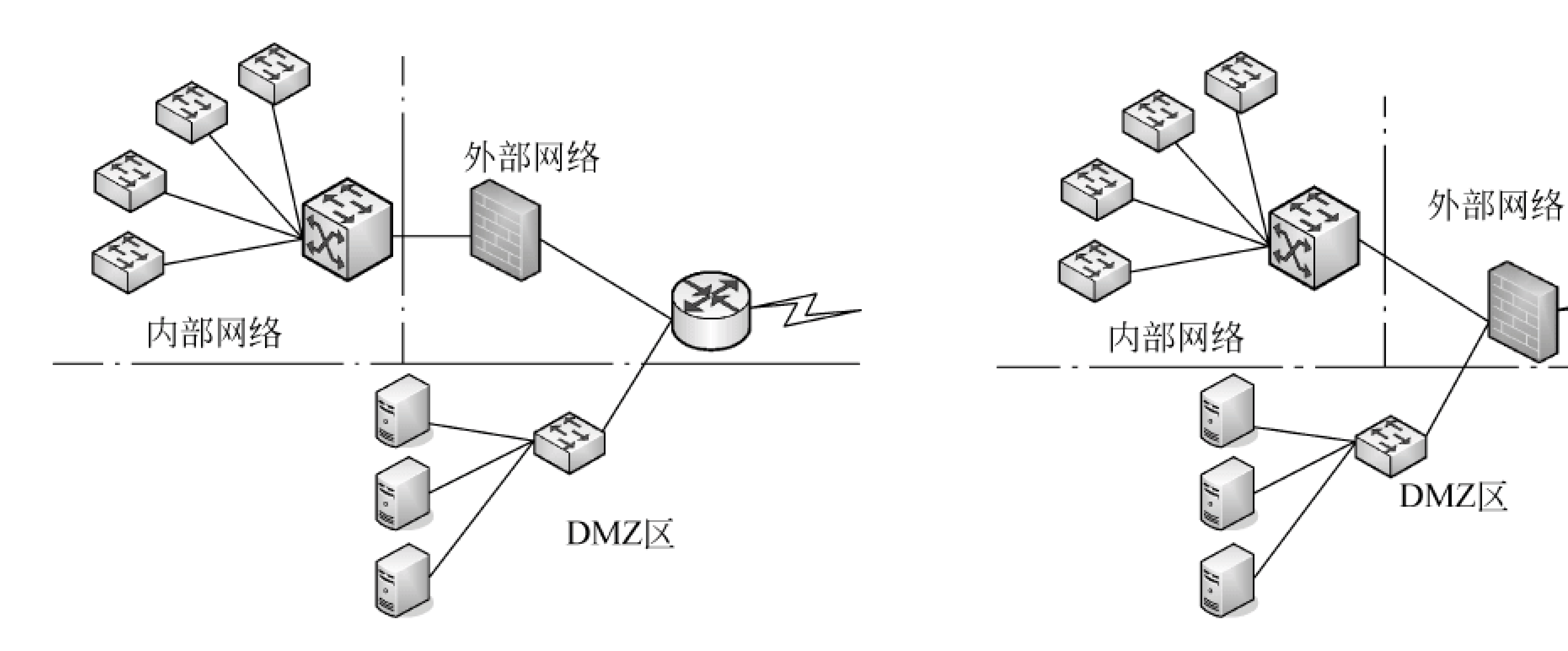


图 12-5　存在边界路由器网络连接　　图 12-6　无边界路由器的网络连接

3. 内部网络不同部门之间的连接

这种应用环境就是在一个企业内部网络之间，对一些安全性要求较高的部门(如人事管理或财务管理等)进行隔离保护，使内部网络中敏感部门的资源不被非法访问。在这些部门的网络主机中的数据对于企业来说是非常重要的，它的工作不能完全离开企业网络，但其中的数据又不能随便供网络用户访问。

一种有效的方法就是采用防火墙进行隔离，在防火墙上进行相关的配置(比划分 VLAN 简单许多)。通过防火墙隔离后，尽管同属于一个内部局域网，但是其他用户的访问都需要经过防火墙的过滤，符合条件时才能访问。这类防火墙不仅要通过包过滤来筛选数据包，而且还要对用户身份的合法性(在防火墙中可以设置允许哪些用户访问)进行识别，通常为自适应代理服务器型防火墙；同时它具有日志记录功能，对网络管理员了解网络安全现状及改进非常重要。在如图 12-7 所示的网络中，同是一个企业的内部网络，可以将需要受到保护的重要部门和一些服务器通过防火墙连接至其他网络。

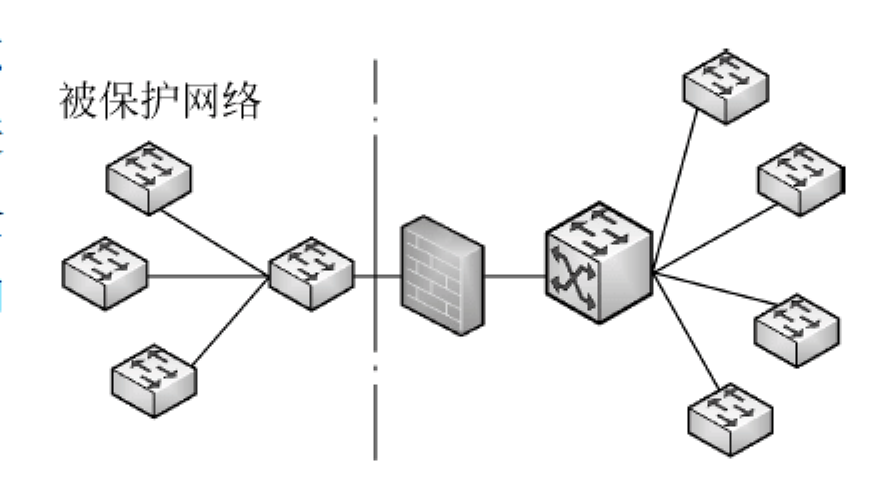


图 12-7　连接内部子网络

4. 用户与中心服务器之间的连接

对于一个服务器中心而言，大多数的服务器都

需要对第三方(合作伙伴或 Internet 用户等)开放,但是所有这些服务器分别属于不同用户所有,其安全策略也各不相同。如果把它们都定义在同一个安全区域中,显然不能满足各用户的不同需求。这时,就可以按不同安全策略保护这些服务器。根据实施方式的不同又可以分为以下两种网络环境。

(1) 每台服务器单独配置独立的防火墙

这种方法是最容易实现的也是最直观的,但这种方案无论从经济上,还是从使用和管理的灵活可靠性上都不是最好的。一则需要购买与托管代理服务器数据一样多的防火墙,对托管中心来说投资非常大;二则托管中心管理员面对这么多防火墙,其管理难度可想而知。

(2) 配置虚拟网络防火墙

这主要是利用三层交换机的 VLAN 功能,先在三层交换机上将有不同安全要求的服务器划分至不同的 VLAN。然后,借助对高性能防火墙模块的 VLAN 子网配置,将防火墙划分为多个虚拟防火墙,如图 12-8 所示。这种方案虽然配置较为复杂,但配置完成后,随后的使用和管理将相当方便,就像用交换机管理多个 VLAN 子网一样来管理每个用户服务器,而且该方案在现实中比较经济可行。

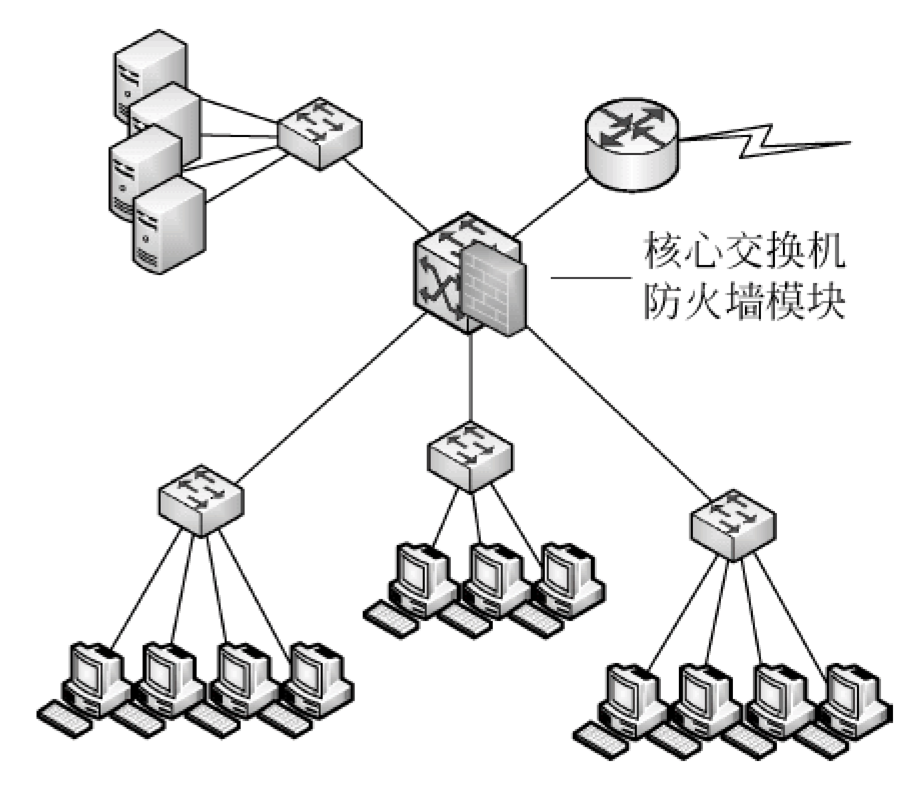


图 12-8　虚拟防火墙

提示:借助三层交换机或路由器内置的防火墙模块,也可以为不同的用户 VLAN 配置不同的安全策略,从而将网络攻击限制在不同的 VLAN 中,从而保证整个网络的安全。

12.2.2　入侵检测系统设计

IDS 一般位于内部网的入口处,安装在防火墙的后面,用于检测入侵和内部用户的非法活动,提供对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前进行拦截和响应入侵处理。它可在不影响网络性能的情况下对网络进行监听,从而实现对网络的保护。

1. IDS 位置

IDS 在交换式网络中一般选择以下位置。

(1) 尽可能靠近攻击源。

(2) 尽可能靠近受保护资源。

这些位置通常在以下位置。

(1) 服务器区域的交换机上(如图 12-9 所示)。

(2) Internet 接入路由器之后的第一台交换机上。

(3) 重点保护网段的局域网交换机上。

在实际的使用中,大多数入侵检测的接入方式,都是采用 by-pass(旁路)方式来侦听网络上的数据流。所以,这就限制了 IDS 本身的阻断功能。IDS 只有靠发阻断数据包来阻断当前行为,并且 IDS 的阻断范围也很小,只能阻断建立在 TCP 协议基础之上的一些行为,如 Telnet、FTP 和 HTTP 等,而对于一些建立在 UDP 基础之上的一些行为就无能为力了。因

为防火墙的策略都是事先设置好的，无法动态设置策略，缺少针对攻击的必要灵活性，不能更好地保护网络的安全。所以 IDS 与防火墙联动的目的就是更有效地阻断所发生的攻击事件，从而使网络隐患降至较低限度。

2. IDS 与防火墙联动

防火墙是实施访问控制策略的系统，对流经的网络流量进行检查，拦截不符合安全策略的数据包。IDS 通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，并发出报警。防火墙和 IDS 之间是互补的关系，两者协同工作，如图 12-10 所示。

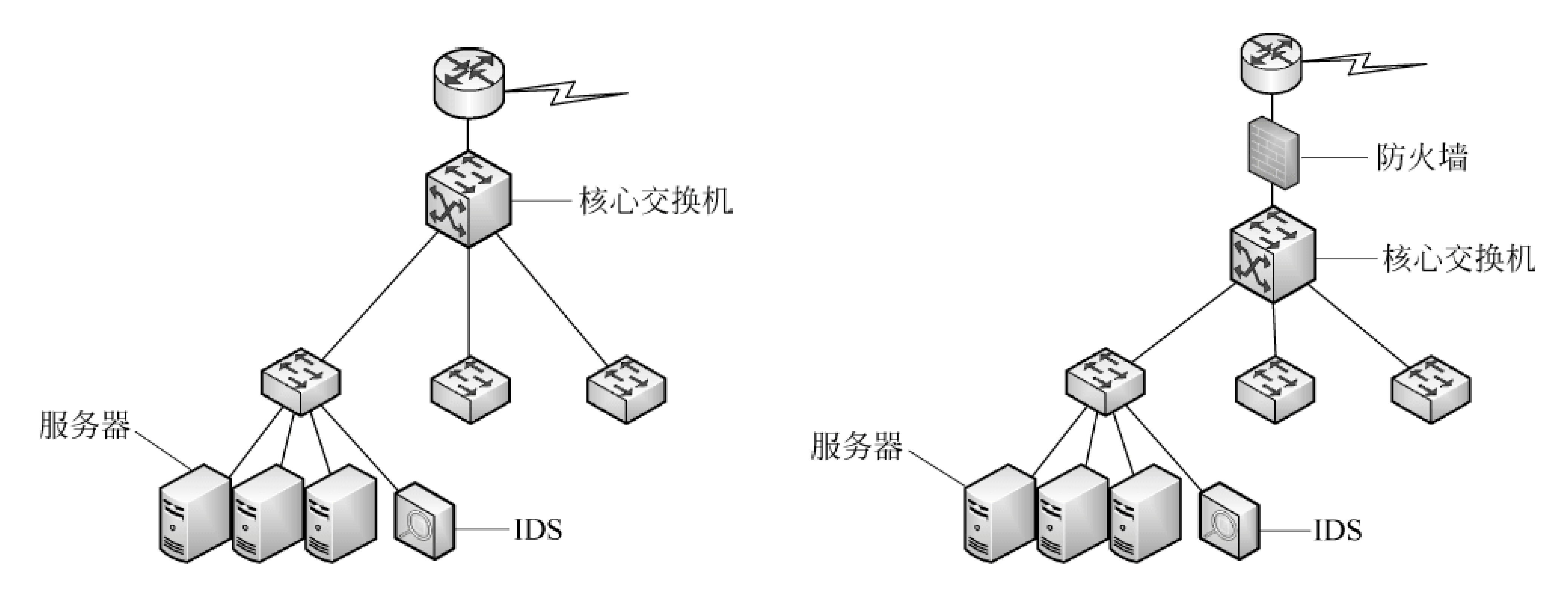


图 12-9　服务器区域的交换机上　　　图 12-10　IDS 与防火墙协同工作

客户一般会在出口部署防火墙来进行访问控制，部署入侵检测系统来检测攻击。但是，防火墙不能有效地检测并阻断夹杂在正常流量中的攻击代码，例如针对 Web 服务的 Unicode 攻击，而蠕虫爆发往往首先让防火墙瘫痪，对于 P2P 下载防火墙同样无能为力。入侵检测系统虽然能够监测到攻击，但是它提供的保护与防火墙联动和 TCP 复位都存在很大的问题，在现实应用中很难起到相应的作用，结果是虽然看到了攻击，但是，仍然让攻击得手了。由此可见，借助防火墙和 IDS 的安全措施并不能完全解决现实问题。

入侵检测系统在捕捉到某一攻击事件后，按策略进行检查，如果策略中对该攻击事件设置了防火墙阻断，那么入侵检测系统就会发给防火墙一个相应的动态阻断策略，防火墙根据该动态策略中的设置进行相应的阻断。阻断的时间、阻断时间间隔、源端口、目的端口、源 IP 和目的 IP 等信息，完全依照入侵检测系统发出的动态策略来执行。一般来说，用户的防火墙与 IDS 并不是同一家的产品，因此在联动的协议上面大都遵从 OPSEC 或者 TOPSEC 协议进行通信。不过，也有某些厂家自己开发相应的通信规范。总的来说，联动有一定效果，但是稳定性不理想。攻击者可以利用伪造的包信息让 IDS 错误判断，进而错误指挥防火墙将合法的地址无辜屏蔽掉。

TCP 重置的缺陷如下。

(1) 只对 TCP 连接起作用。

(2) IDS 向攻击者和受害者发送 TCP Reset 命令，IDS 必须在 40 亿字节的范围内猜测到达受害者时的序列号数，以关闭连接。这种方法在实际上是不可实现的。

(3) 即使 IDS 最终猜测到了到达受害者的序列号，关闭了连接，攻击实际上已经对受害者产生了作用。

IDS 与防火墙联动的缺点如下。

(1) 使用和设置上复杂,影响 FW 的稳定性与性能。

(2) 阻断来自源地址的流量,不能阻断连接或单个数据包。

(3) 黑客盗用合法地址发起攻击,造成防火墙拒绝来自该地址的合法访问。

(4) 可靠性差,实际环境中没有实用价值。

因为诸多不足,在目前而言,IDS 主要起的还是监听记录的作用。用个比喻来形容:网络就好比一片黑暗,到处充满着危险,冥冥中只有一个出口。IDS 就像一个手电筒,虽然手电筒不一定能照到正确的出口,但有总比没有要好一些。称职的网管,可以从 IDS 中得到一些关于网络使用者的来源和访问方式,进而依据自己的经验进行主观判断(注意,的确是主观判断。例如,用户连续 ping 了服务器半个小时,到底是意图攻击,还是无意中的行为?这都依据网络管理员的主观判断和网络对安全性的要求来确定对应方式)对 IDS 的选择,与上面谈到防火墙的选择类似,根据自己的实际要求和使用习惯,选择一个自己够用的、会使用的就足够了。

12.2.3　入侵防御系统设计

IPS 同防火墙在网络中的连接方式基本相似。不过,也有其较为特殊的方式。通常情况下,依据 IPS 防护的区域不同,而将其连接至不同的位置。

1. 路由防护

路由防护,将 IPS 直接部署至路由器和核心交换机之间,借助网络的边界防护,实现 IPS 和防火墙功能,为整个网络提供网络安全保护,如图 12-11 所示。

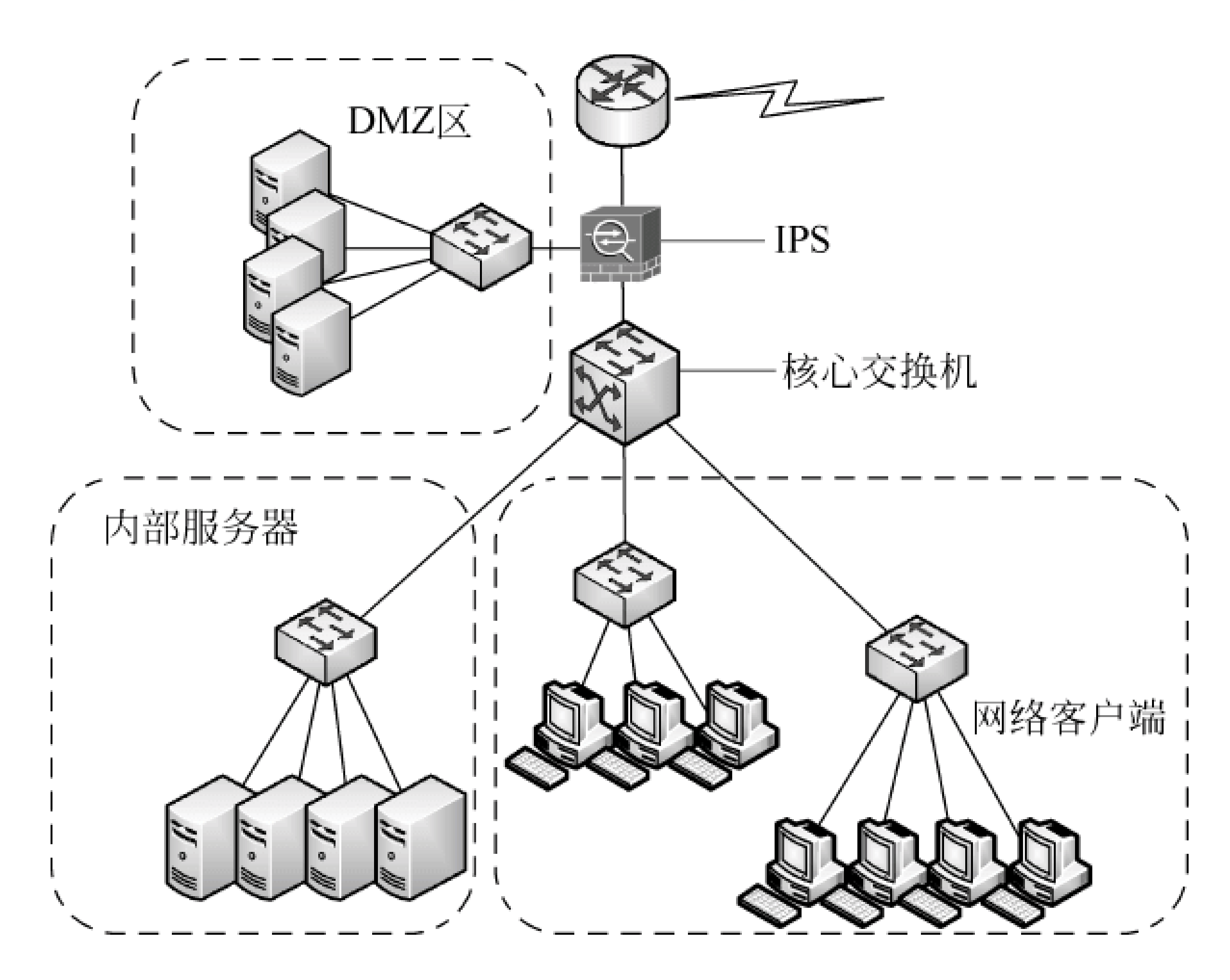


图 12-11　路由防护

2. 交换防护

将 IPS 作为网络核心,采用一进多出或多进多出的方式,实现不同网段相互连接,进行数据交换,同时实现防火墙功能,如图 12-12 所示。

3. 多链路防护

采用多路 IPS 的连接方式,一路 IPS 防护一个 ISP 接入,各路 IPS 相互独立,彼此之间没有数据交换,互不干扰,如图 12-13 所示。

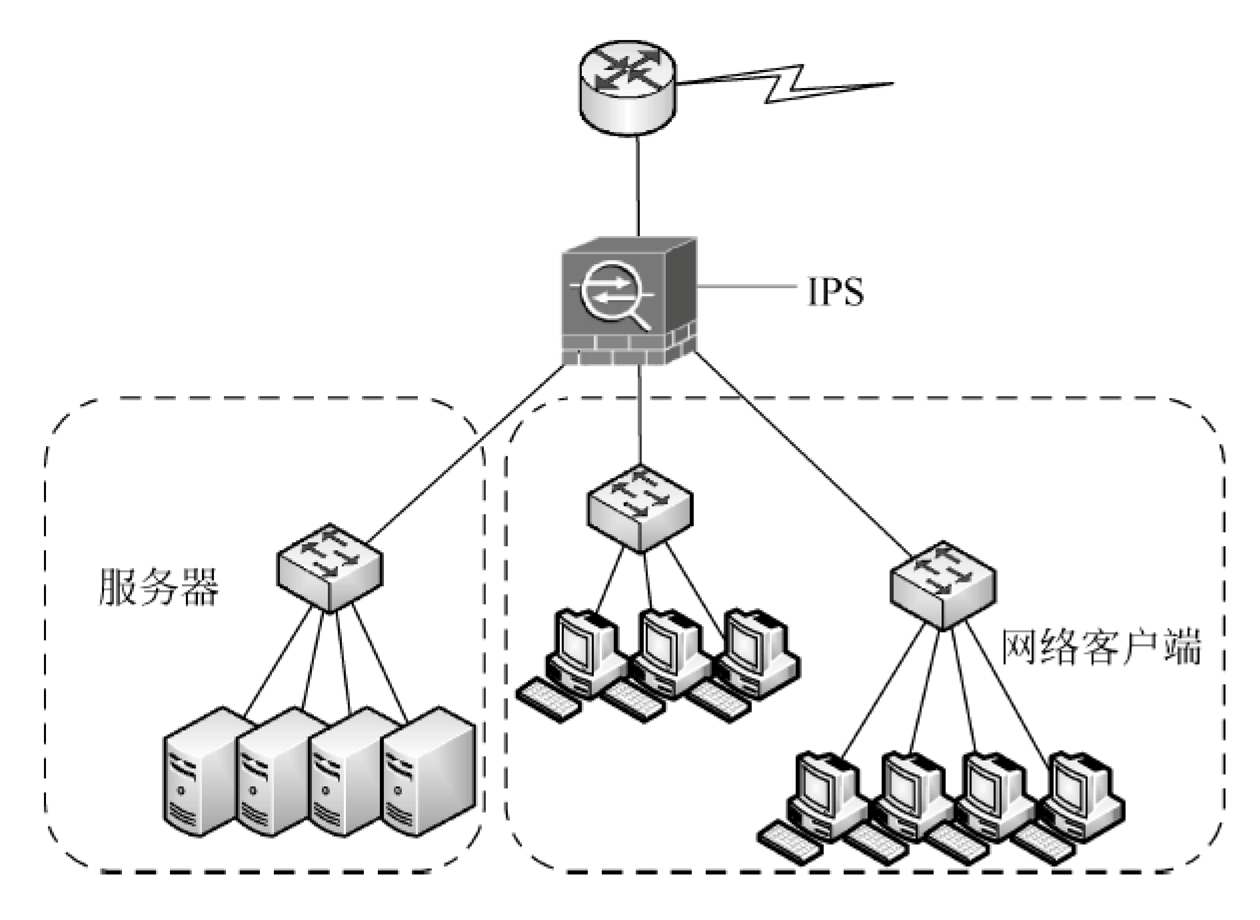


图 12-12 交换防护

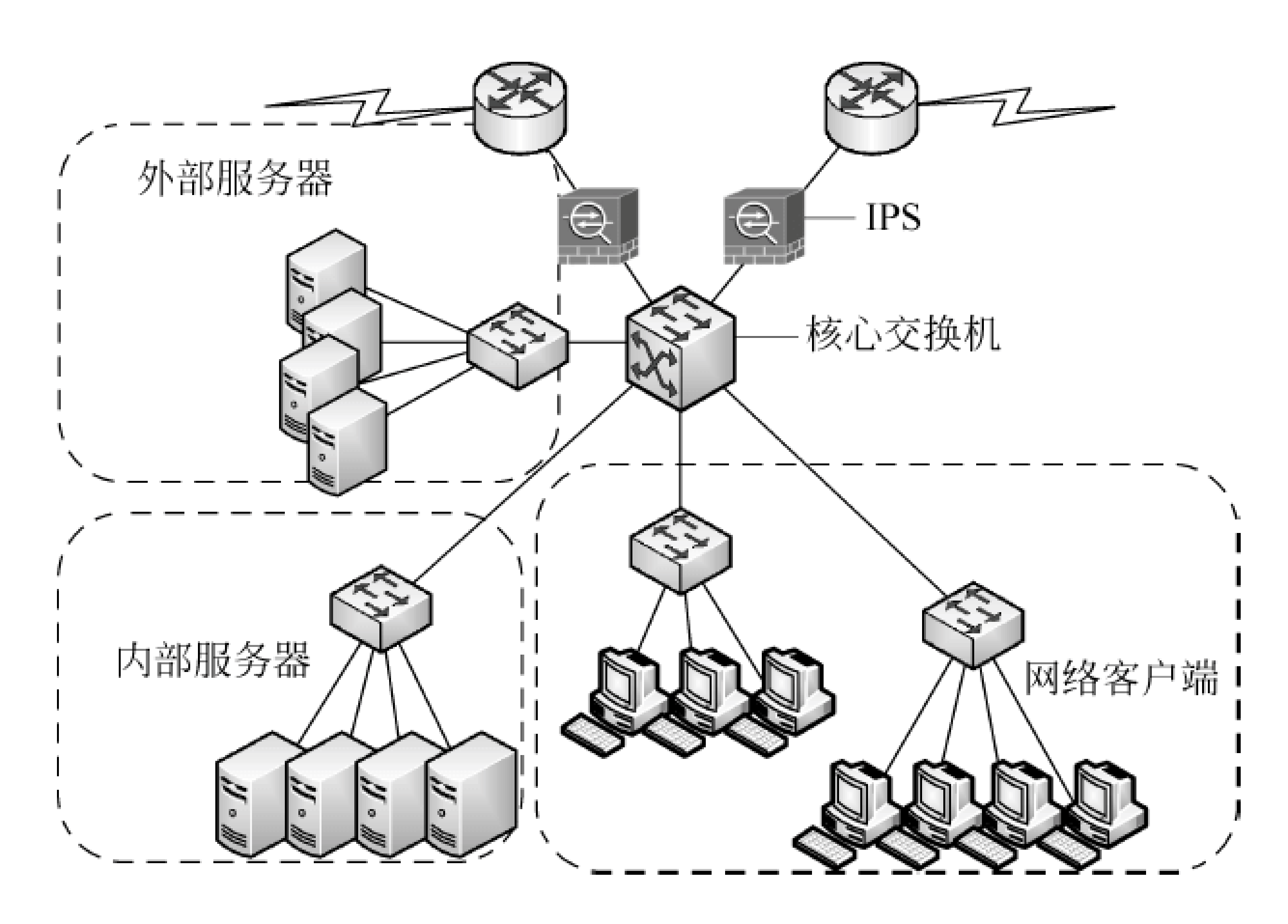


图 12-13 多链路防护

4. 混合防护

多种模式分层防护，监控与防护相结合，更完善。在线 NIPS 模式与旁路 NIDS 模式相配合，如图 12-14 所示。

12.2.4 综合安全设计

为了充分发挥各种安全设备的优点，以取得最好的网络安全效果，可以将不同的安全产品应用至不同的网络位置，使其安全功能相互搭配，从而发挥每个设备的最佳安全效能，实现无缝的网络安全。

通常情况下，将 IPS 置于网络总出口，实现网络入侵过滤；IDS 旁路于服务器群组的 Uplink 端口，侦测对网络服务器发动的攻击；核心交换机集成防火墙模块，实现虚拟防火墙与 IDS 的互动，交换机和路由器启用 IOS 防火墙。网络拓扑结构如图 12-15 所示。

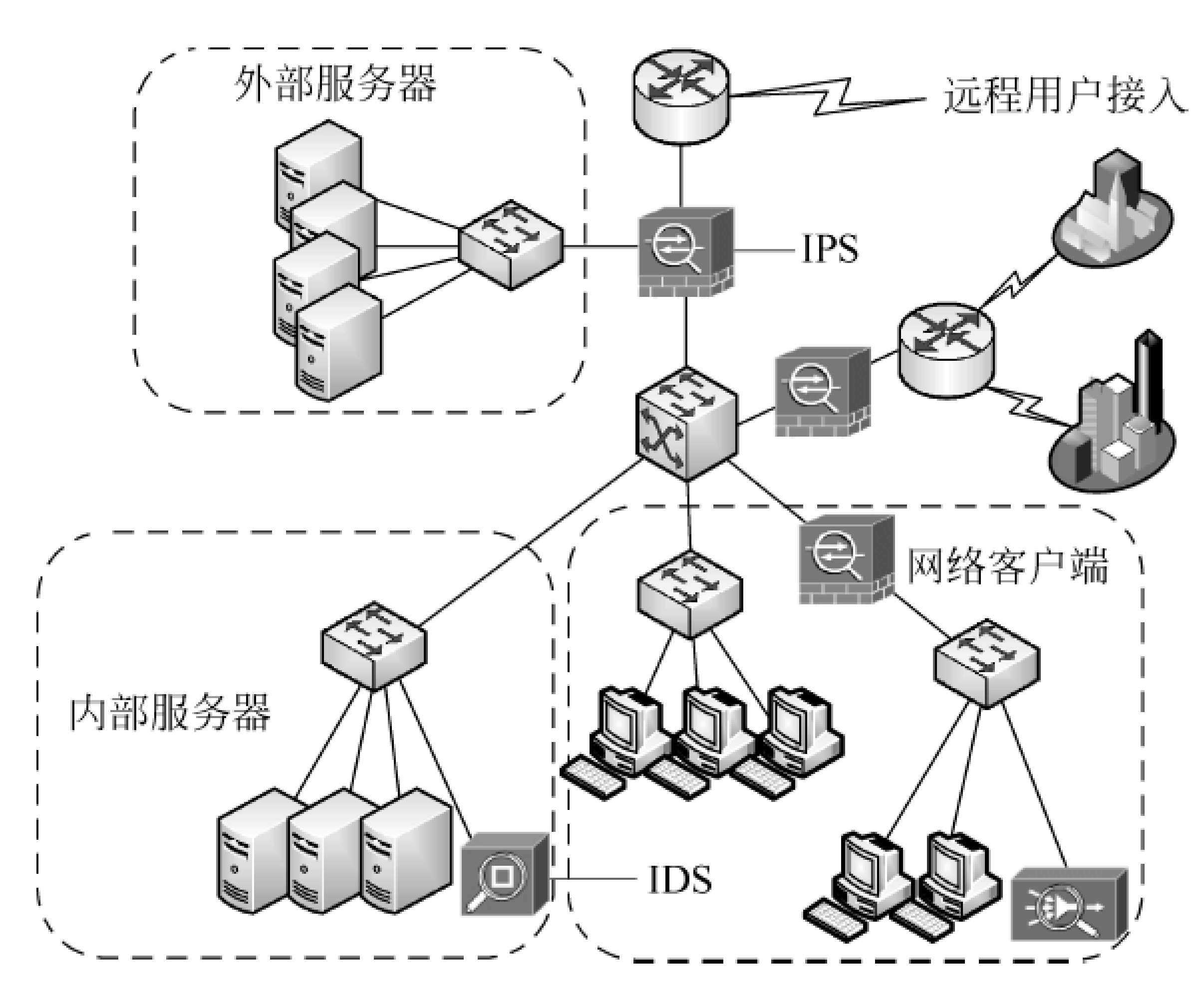


图 12-14　混合防护

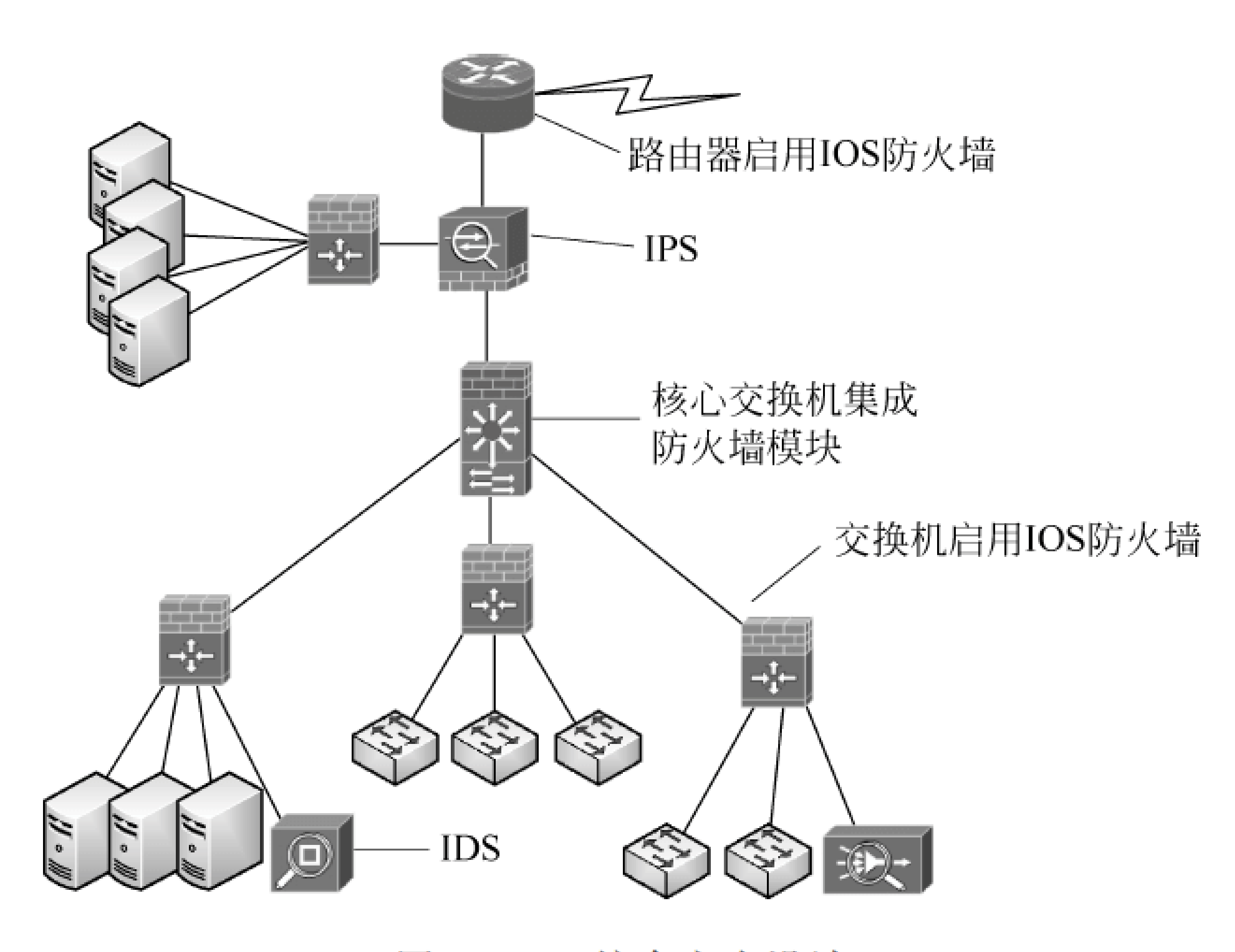


图 12-15　综合安全设计

12.2.5　知识链接：网络防火墙、IDS 与 IPS

1. 网络防火墙——Cisco PIX 和 ASA

很多年来，Cisco PIX 一直都是 Cisco 最具代表性的防火墙。PIX 防火墙使用 PIX 操作系统。虽然 PIX 操作系统和 Cisco IOS 看起来非常接近，但是，彼此之间还是有着较大的差异性。与之相比，Cisco ASA 是 Cisco 系列中全新的防火墙和反恶意软件安全产品，允许用户根据网络环境选择适合自己的安全产品，适应领域更广。

尽管 PIX 是一款非常优秀的防火墙，但是，由于安全威胁日新月异，因此，仅仅使用一台静态数据包过滤防火墙来保护网络已经远远不够了。对于网络而言，新的安全威胁层出不穷——包括病毒、蠕虫、大量应用软件（例如 P2P 软件、网络游戏、即时通信软件等）、网络欺诈，以及应用程序层面的攻击等。

如果一台设备可以应付多种威胁，就称其提供了 Anti-X 能力，或者说它提供了“多重威胁（multi-threat）”防护，但是，PIX 恰恰无法提供这种层次的防护。显然，大家都不希望采取安装一台 PIX 进行静态防火墙过滤，同时，再使用一些其他的工具来防护其他威胁的办法。因此，用户更迫切需要一台“集所有功能于一身”的设备——或是采用一台 UTM（统一威胁管理）设备。

ASA 恰好针对这些不同类型的攻击提供了防护，甚至比一台 UTM 设备更强劲、更有效。不过，若欲成为一台真正的 UTM，还需要装一个 CSC-SSM 模块（Content Security and Control Security Service，内容安全以及控制安全服务）。该模块在 ASA 中提供 Anti-X 功能，如果没有 CSC-SSM，那么 ASA 的功能看起来会更像一台 PIX。

在购置安全设备时，建议选择 ASA 而不是 PIX。首先，ASA 的价格比同样功能的 PIX 要低。其次，选择 ASA 就意味着选择了更新更好的技术。

对于已经在使用 Cisco PIX 的用户而言，Cisco 已经提供了一个迁移指南，可以解决从 Cisco PIX 迁移到 ASA 上的问题。由于厂商往往是提供从老产品向新产品的迁移指南，而不是相反，可见，Cisco 终止 PIX 的日子正离我们越来越近。

提示：面对 Internet 上五花八门的不同威胁，无法再简单地像以往那样有了一套防火墙就万事大吉了。对完整的防护措施而言，一个多重防护的方法必不可少。虽然 ASA 的确是很好的一个选择，但是这也并不意味着它是唯一选项。许多生产商（特别是国内安全厂商）都提供了很好的产品，因此，可选择的余地还是很大的。

2. IDS 与 IPS 比较

IPS 是在 IDS 的基础上发展出来的，IDS 是一种网络安全系统，当有敌人或者恶意用户试图通过 Internet 进入网络甚至计算机系统时，这种系统可以检测出来，并进行报警，通知管理员采取措施进行响应。IPS 是 IDS 技术的一种新发展趋势，IPS 技术在 IDS 监测的功能上又增加了主动响应的功能，一旦发现有攻击行为，立即响应，主动切断连接。

提到 IPS，人们常常会谈到一个公式，IPS＝Firewall＋IDS。也有文献认为，将 IDS 的传感器置于网络通信线路之内（In-line），让所有网络通信量必须通过它，就得到了一台 IPS。这两种看法均有偏颇之处，但是，却殊途同归地道出了一个事实——IPS 来自 IDS。概括地讲，IPS 与 IDS 的区别如下。

（1）部署位置不同。IPS 部署在链路上，对于来自外部的威胁，例如蠕虫传播、木马、黑客攻击等，IPS 直接阻断，不让它进入客户网络。对于来自内部的威胁，例如蠕虫传播、黑客攻击等，IPS 阻断攻击，保护服务器。而 IDS 则是部署在需要进行特殊保护的分支网络中。

（2）检测方式不同。IDS 采用被动侦听方式，所以响应能力很有限，如发送 TCP Reset 包终止会话时往往可能已经为时太晚。IPS 采用了多种检测技术，特征检测可以准确检测已知的攻击。IPS 将检查入网的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包进入内部网络。

（3）处理攻击的方式不同。IDS 只能报警而不能有效采取阻断措施的设计理念，也不能满足用户对网络安全日益增长的需求。充其量，IDS 只能与防火墙联动的方式来解决部分网络攻击。IPS 的拦截行为与其分析行为处在同一层次，能够更敏锐地捕捉入侵的流量，并能将危害切断在发生之前，这种主动防御的响应能力正是网络安全真正需要的。

12.3　配置安全设备

网络是否安全，在很大程度上取决于安全设备的配置，只有将安全设备配置得足够安全，才能使其更好地为网络服务，使网络不会被外部计算机入侵，进而保障网络的稳定。

12.3.1　Cisco ASA 连接策略

Cisco ASA 的功能非常丰富，不仅是一台网络防火墙，还是一台入侵检测设备、一台入侵防御设备、一台 VPN 设备，甚至一台路由器。因此，Cisco ASA 的应用领域非常广泛，可以部署于网络中的每个位置。

实现与 Internet 的安全连接，是 Cisco ASA 最基本和最典型的应用，可以为网络内部客户提供安全的网络连接（如图 12-16 所示）。当然，在 Cisco ASA 之后，还可以再加一台交换机，以实现多用户的网络接入。

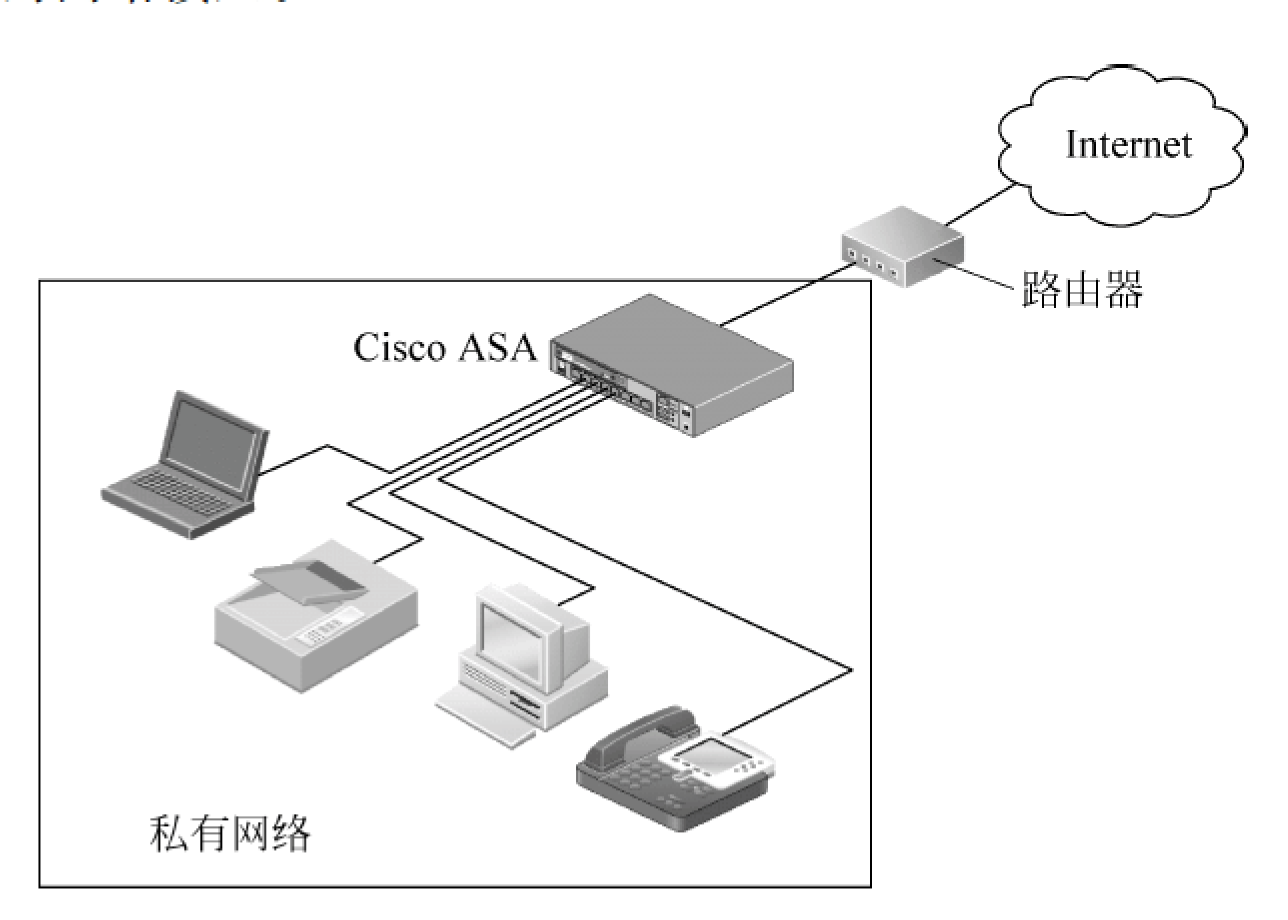


图 12-16　安全 Internet 连接

同时，Cisco ASA 还支持虚拟防火墙技术，因此，一台普通的 Cisco ASA 5500 系列产品，就可以作为至少两台网络防火墙使用，实现双 Internet 链路的负载均衡（如图 12-17 所示）。真可谓一分投入，双倍收益。

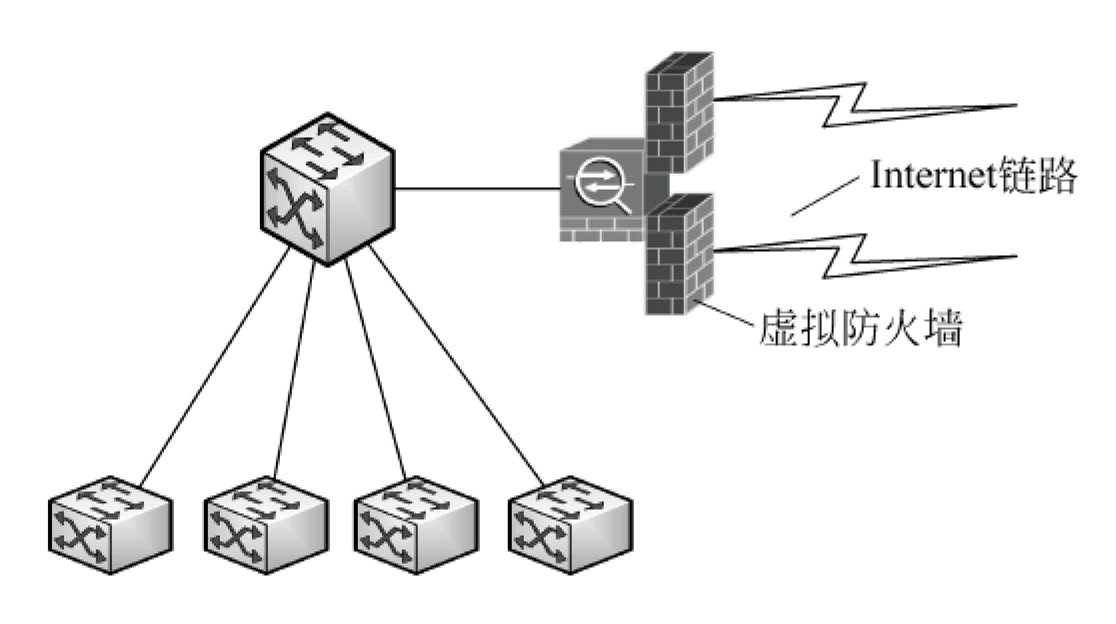


图 12-17　虚拟网络防火墙

借助 Cisco ASA 提供的 DMZ 区域，还可以安全地发布网络服务器(如图 12-18 所示)，从而使服务器发布和内部网络安全得到了很好的平衡。

Cisco ASA 还是一款性能非常强劲的 VPN 服务器，支持 SSL VPN 和 IPSec VPN，因此，可以为远程用户提供安全、廉价、高速的访问服务(如图 12-19 所示)，无论何时何地，都可以安全地访问内部网络中的资源。

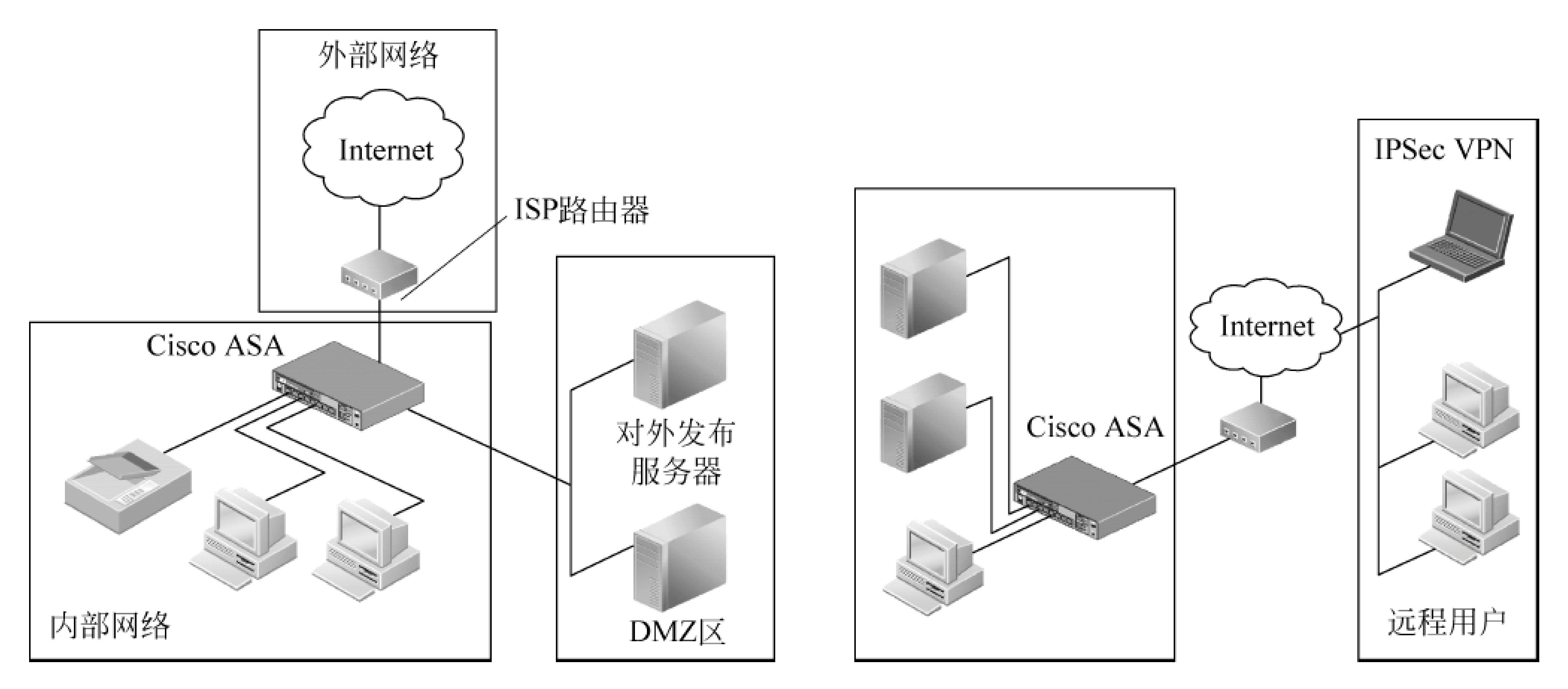


图 12-18 发布网络服务器　　图 12-19 VPN 远程安全访问

当然，由于 Cisco ASA 性能强劲，因此，用于实现部门与分支机构之间的 VPN 连接也不成问题(如图 12-20 所示)，从而借助 Internet 的廉价链路，达成机构内部之间的安全通信与数据交换。

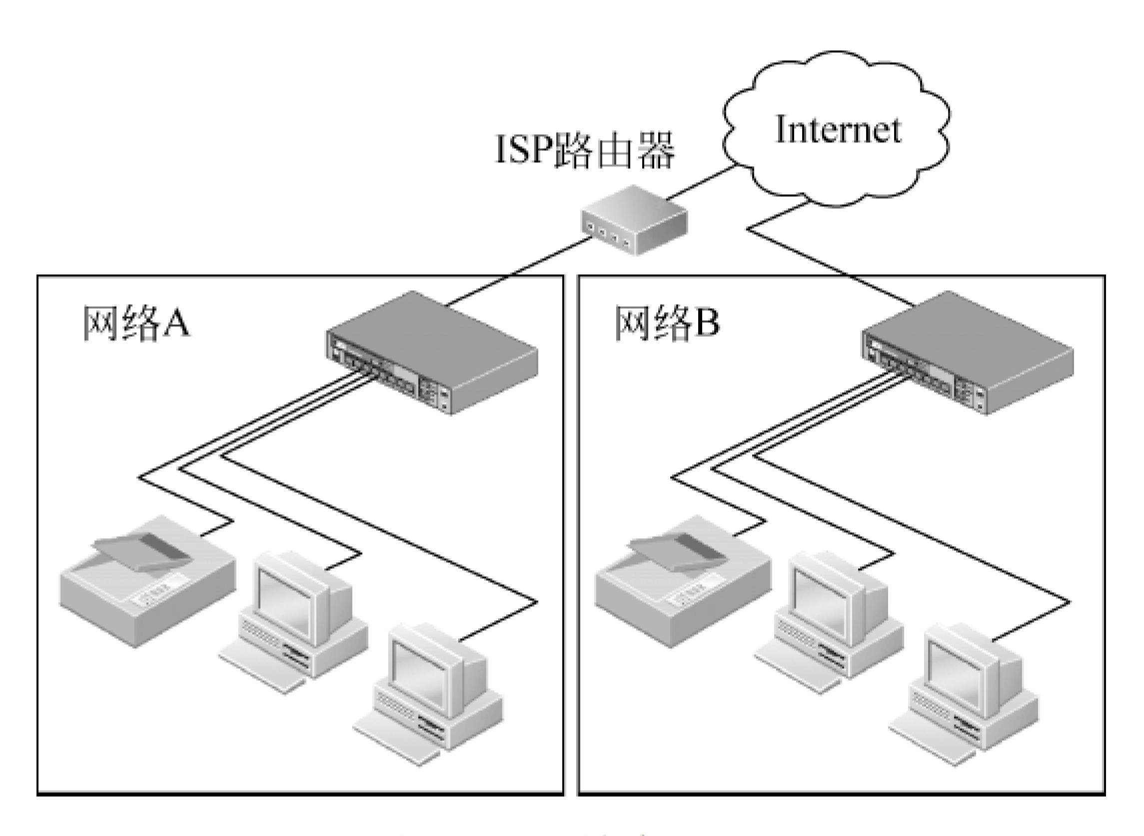


图 12-20 站点 VPN

总之，Cisco ASA 最常见的应用非常丰富(如图 12-21 所示)，既可以提供移动用户的远程 VPN 安全接入，又可以与远程网络的 VPN 连接，还可以实现内部网络的安全 Internet 接入，以及服务器的安全发布。

12.3.2 Cisco ASDM 初始化

1. 安装前的准备

在开始运行 Startup Wizard(启动向导)之前，首先需要执行以下操作。

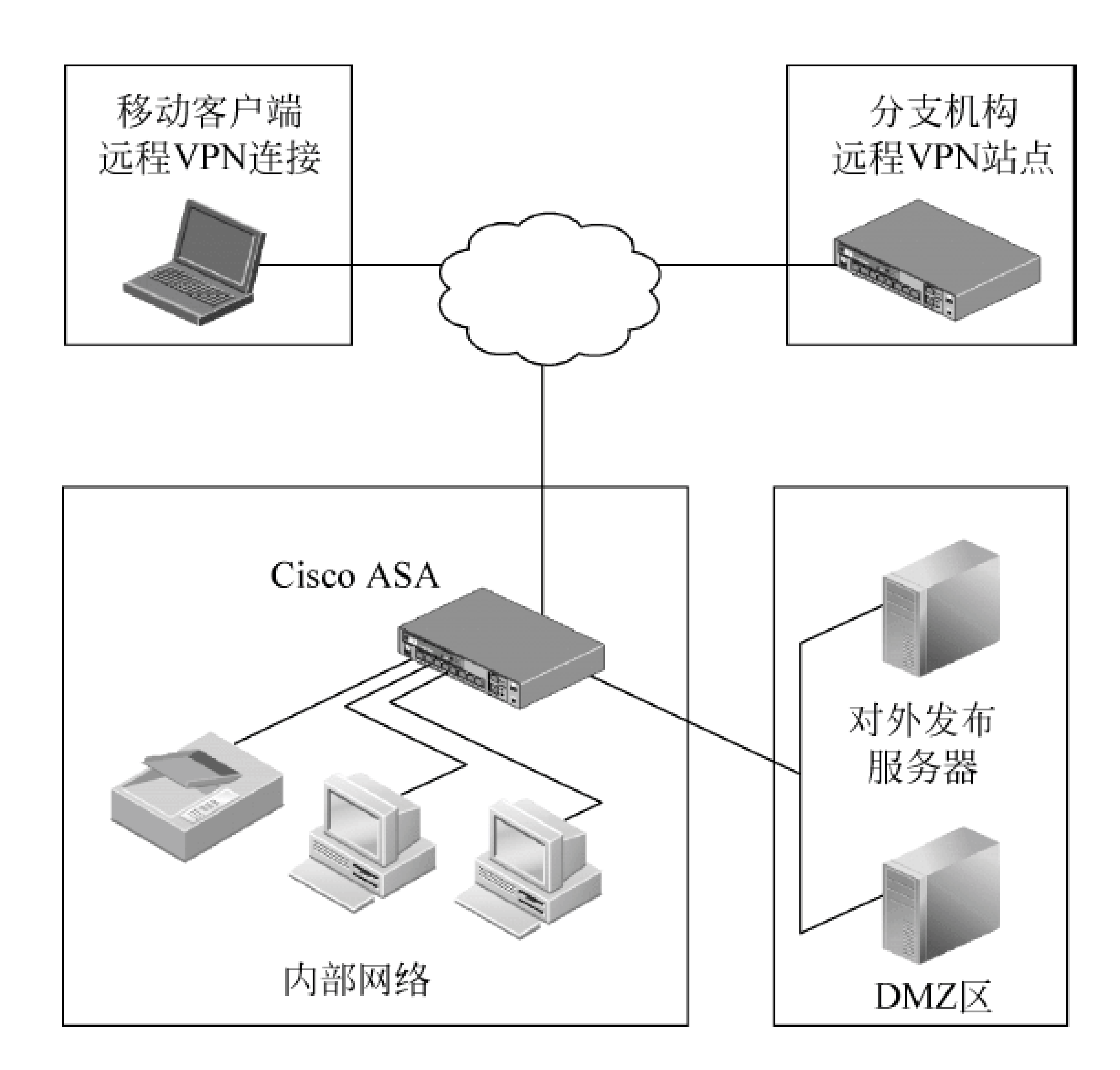


图 12-21　Cisco ASA 典型应用

(1) 获得一个 DES 许可证或 3DES-AES 许可证。

提示：运行 ASDM，必须拥有自适应安全设备的 DES 许可证或 3DES-AES 许可证。

(2) 在 Web 浏览器启用 Java and JavaScript。

(3) 搜集下列信息。

① 在网络中能够识别自适应安全设备的主机名。

② 外部接口、内部接口和其他接口的 IP 地址信息。

③ 用于 NAT 或 PAT 配置的 IP 地址信息。

④ DHCP 服务器的 IP 地址范围。

2. 使用 Startup Wizard

ASDM 使用 Startup Wizard 简单地初始化自适应安全设备，启动向导可以启用自适应安全设备，实现数据在内部接口(GigabitEthernet0/1)和外部接口(GigabitEthernet0/0)的安全传输。

(1) 如果是 ASA 5520 或 ASA 5540，使用跳线将入口 GigabitEthernet0/1 连接到交换机或其他集线设备。如果是 ASA 5510，使用跳线将入口 Ethernet 1 连接到交换机或其他集线设备。然后，在同一台交换机上连接管理用计算机，实现对自适应安全设备的配置。

(2) 配置计算机使用 DHCP 方式，将自动从自适应安全设备获得 IP 地址信息。也可以为计算机指定静态 IP 地址信息，其取值范围为 192.168.1.2 ～ 192.168.1.254，子网掩码为 255.255.255.0，默认网关为 192.168.1.1。

提示：自适应安全设备的内部接口默认被指定为 192.168.1.1。

(3) 如果是 ASA 5520 或 ASA 5540，检查 GigabitEthernet0/1 接口的 LINK LED 指示灯。如果是 ASA 5510，则检查 Ethernet 1 接口的 LINK LED 指示灯。当连接正常时，相应接口的 LINK LED 指示灯应当呈绿色。

(4) 运行 Startup Wizard 启动向导。在配置计算机上运行 Web 浏览器，在地址栏中输

入“https://192.168.1.1/”,并按 Enter 键。

(5) 在相应文本框中输入用户名和密码。需要注意的是,默认密码为空。因此,可以直接按 Enter 键进入。

(6) 单击 Yes 按钮,同意安装数字证书,并在随后的所有确认对话框中全部单击 Yes 按钮即可。

(7) ADSM 启动。从 ASDM 窗口顶端的 Wizards 菜单中,选择 Startup Wizard 选项。

(8) 根据启动向导中的提示,设置自适应安全设备即可。

12.3.3 网络设备集成化管理

对于 Cisco AIP-SSM 的全面管理服务。

(1) 为管理可实现多种防御服务的 Cisco AIP-SSM,提供平稳的集成和支持。

(2) 通过使用威胁识别和准确防御技术,可实现迅速配置、准确攻击监控和网络威胁防御功能,使企业网络免遭蠕虫、间谍软件和其他恶意软件的影响,而且也不会存在丢弃合法流量的风险。

虚拟化安全服务的世界级管理。

(1) 可在单一 Cisco ASA 5500 系列自适应安全设备或 Cisco PIX 安全设备中迅速创建多个安全环境(虚拟防火墙),每个环境有自己的一套安全策略、逻辑接口和管理域。

(2) 使企业能方便地将多个防火墙整合到一个安全设备或故障恢复对中,且能分别管理每个虚拟环境。

(3) 使服务供应商可以通过冗余设备,提供永续的多租户防火墙服务。

12.3.4 安全策略设置

在安全策略设置上,通常包括以下几种设置。

(1) 内到外全部允许,外到内全部拒绝。

(2) 内到外和外到内都要做 ACL 控制、映射、NAT。

(3) 设置 IPSec、L2TP、SSL VPN。

当今的安全威胁需要用新的方法消除,要实现全面的应用安全性,需要提高对整个网络中的应用的敏感性,而不是用一种方法保护网络中的所有应用。每种应用都需要一组通用服务,以及其他应用专用检测服务。这些应用检测服务必须满足当今网络的性能和服务要求。所有要求都必须与清晰、全面的架构密切相连,以便灵活地部署和实施应用安全策略。Cisco ASA 5500 系列自适应安全设备不但能提供新型应用保护方法,还能保护关键业务应用的可用性和完整性。

Cisco ASA 5500 系列通过自适应识别和防御架构,进一步提高了网络的安全性和策略控制。利用遍及所有主要网络协议的应用安全检测引擎,Cisco ASA 5500 系列允许部署全面的应用安全策略。每种检测引擎都监控应用流,并能够标示和阻止针对特定协议的非法操作。图 12-22 所示为安全策略的设置。

12.3.5 配置 DMZ

DMZ 网络拓扑结构(如图 12-23 所示)具有以下特征。

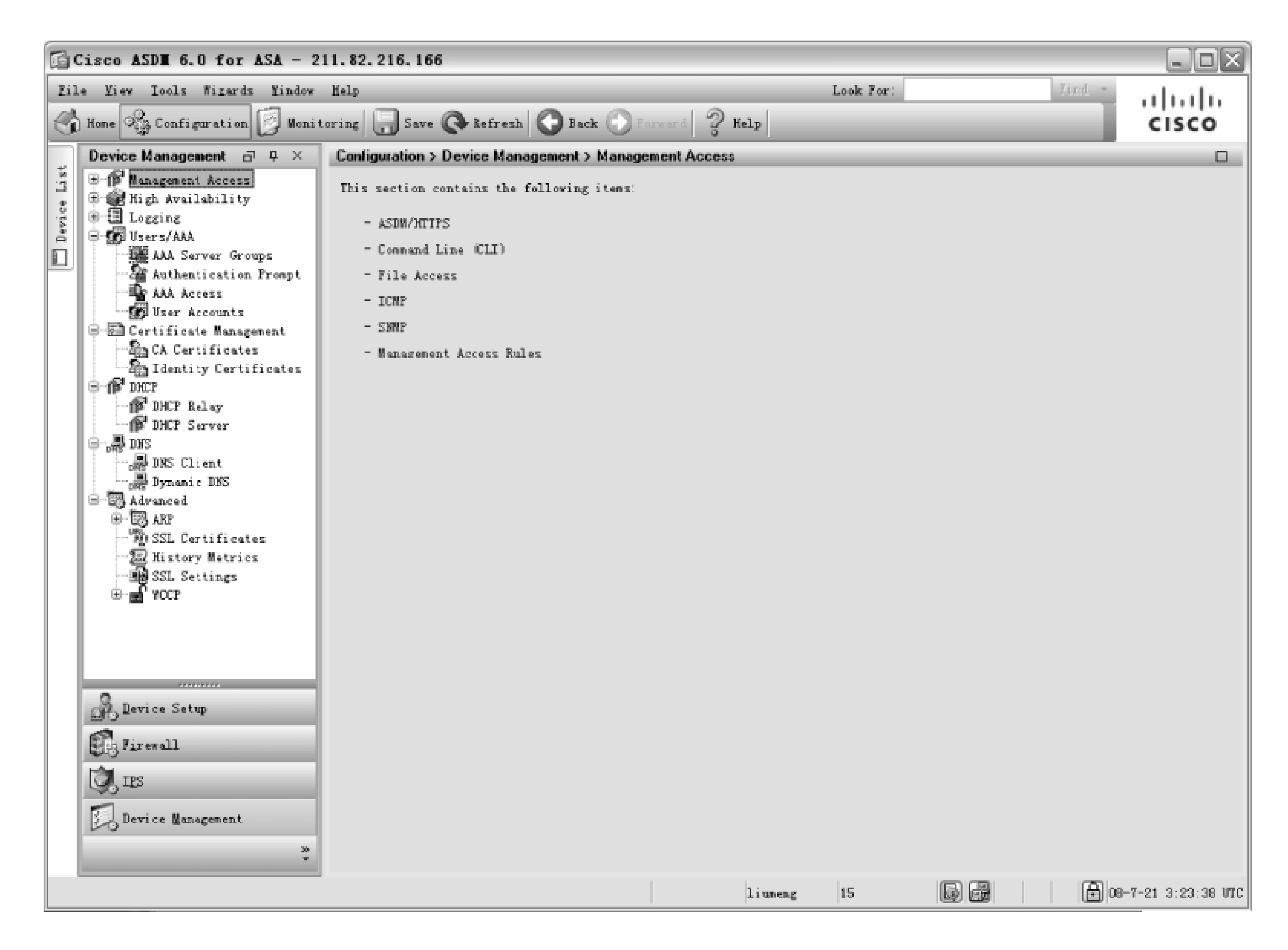


图 12-22　安全策略

(1) Web 服务器连接至安全设备的 DMZ 接口。

(2) HTTP 客户端位于私有网络，可以访问位于 DMZ 中的 Web 服务器，并且可以访问 Internet 中的设备。

(3) Internet 中的 HTTP 客户端允许访问 DMZ 区的 Web 服务器，除此之外的其他所有的通信都被禁止。

(4) 网络有两个可路由的 IP 地址可以被公开访问：安全设备外部端口的 IP 地址为 209.165.200.225，DMZ 中 Web 服务器的公开 IP 地址为 209.165.200.226。

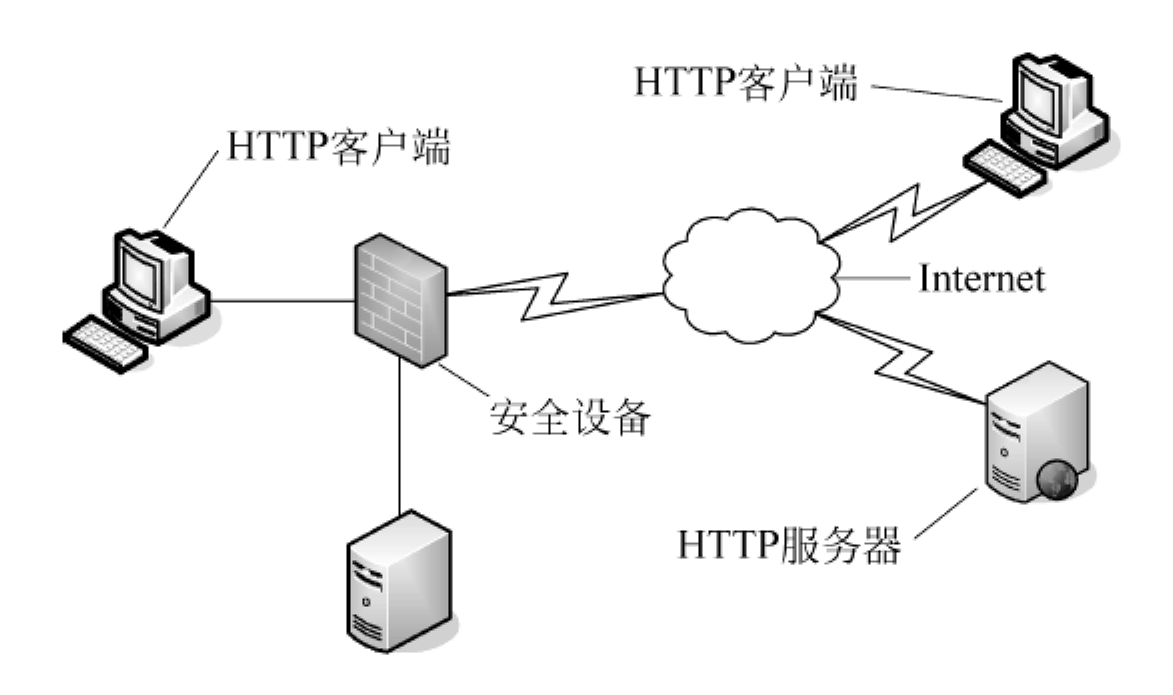


图 12-23　DMZ 网络拓扑结构

1. 运行 ASDM

(1) 打开 Web 浏览器，在地址栏中输入欲配置和管理的安全设备的 IP 地址 https://211.82.216.166，显示如图 12-24 所示的 Cisco ASDM 6.0 对话框。

(2) 单击 Run ASDM 按钮，显示如图 12-25 所示的 Cisco ASDM 程序的登录窗口。根据实际情况，输入配置和管理的安全设备的 IP 地址、用户名和密码。

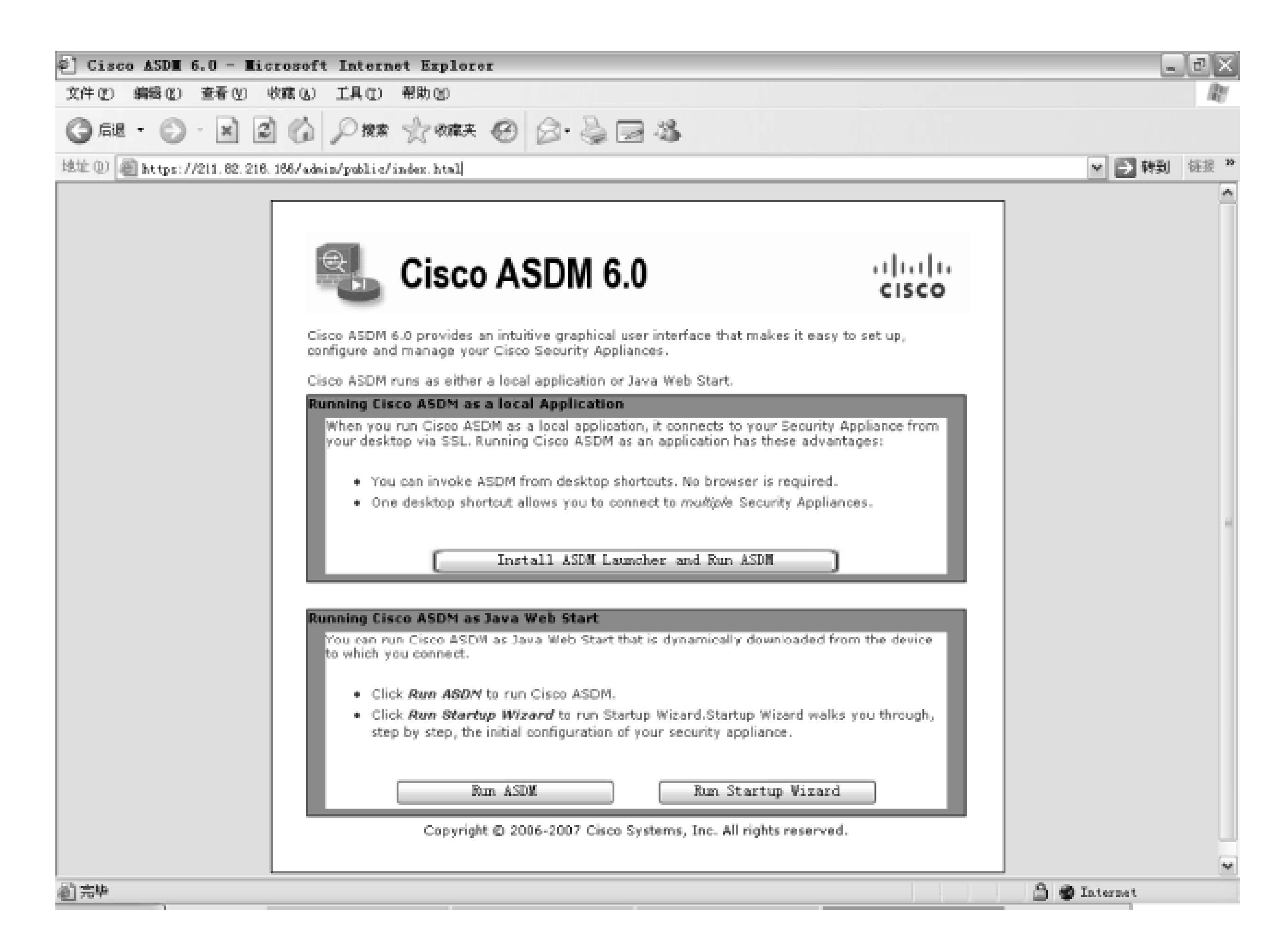


图 12-24　Cisco ASDM 6.0 对话框



图 12-25　Cisco ASDM 登录窗口

（3）单击 OK 按钮，显示如图 12-26 所示的 Cisco ASDM 主窗口。

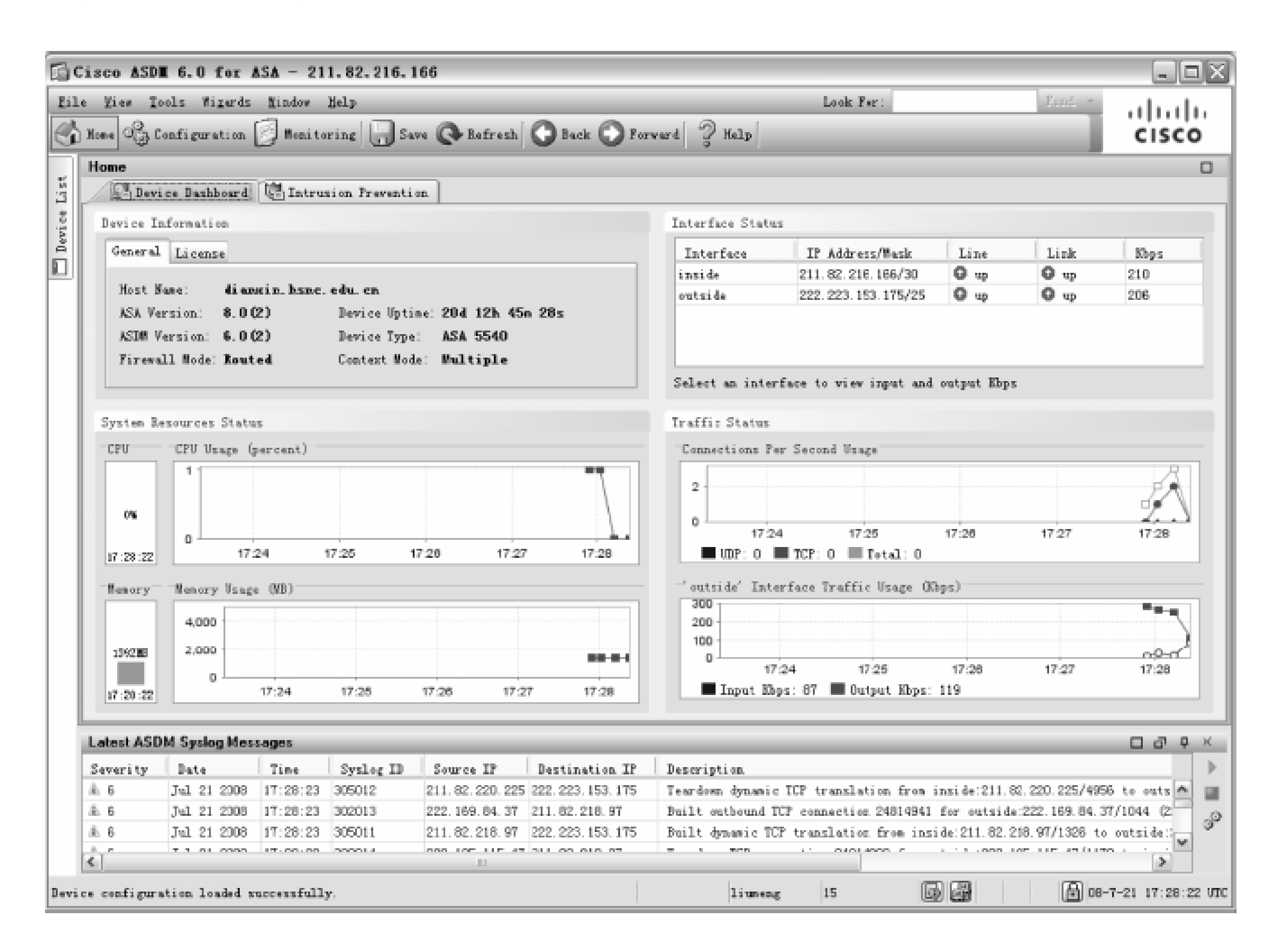


图 12-26　Cisco ASDM 主窗口

2. 为 NAT 创建 IP 地址池

安全设备使用网络地址转换和端口地址转换，防止内部 IP 地址暴露在外部网络或 Internet。这里介绍如何为 DMZ 接口和外部接口创建一个可以被转换的 IP 地址池。

提示：一个 IP 地址池可以同时包含 NAT 条目和 PAT 条目，也可以包含 1 个以上接口的条目。

（1）在 ASDM 窗口工具栏，单击 Configuration 图标，在左侧栏中单击 Firewall 选项中的 NAT Rules 规则，显示如图 12-27 所示界面。

（2）在右侧栏中选择 Global Pools 选项卡，单击 Add 按钮，显示如图 12-28 所示的 Add Global Address Pool 对话框，为 DMZ 接口创建一个新的全局地址池。

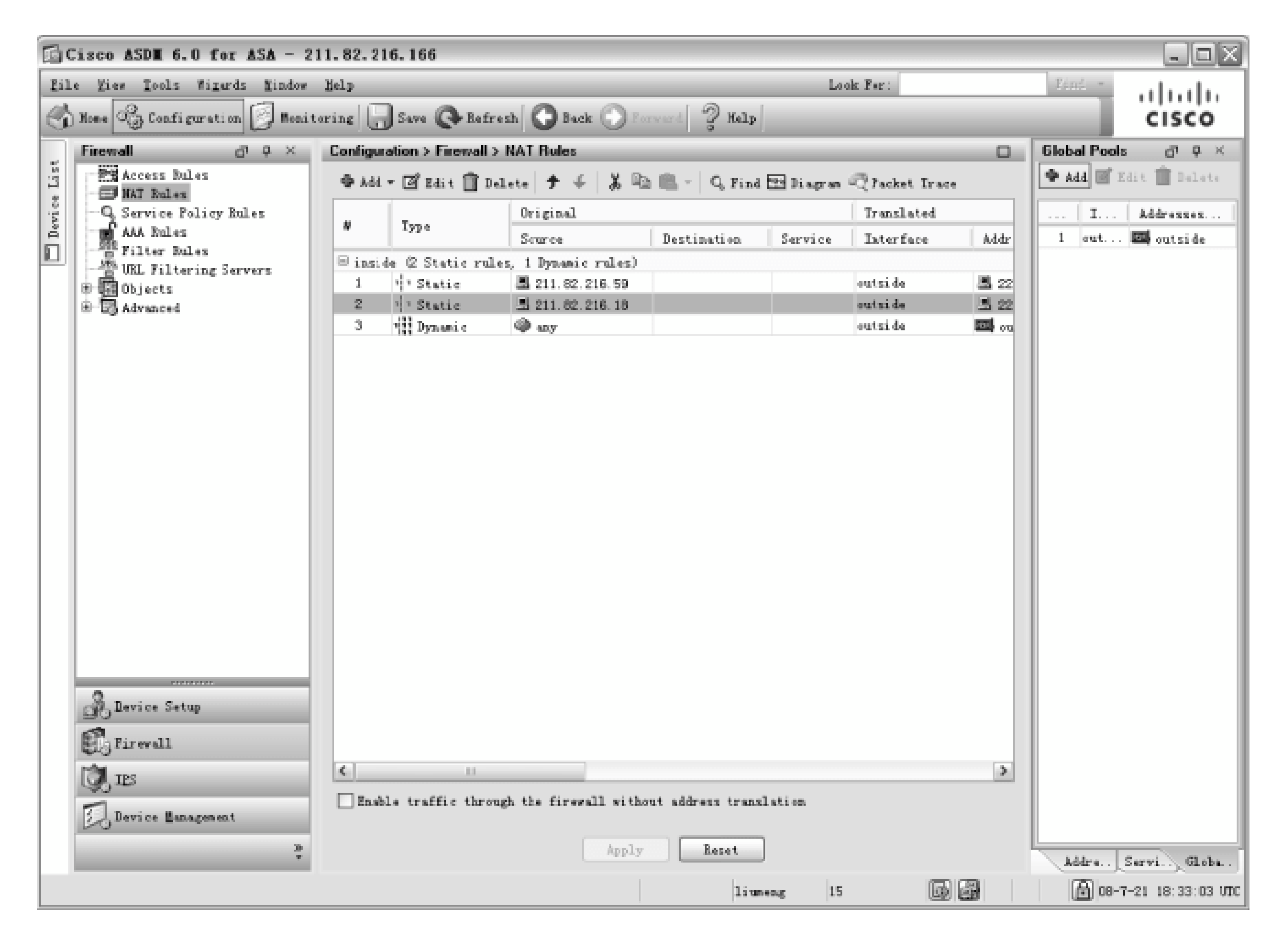


图 12-27　NAT Rules 规则

（3）从 Interfaces 下拉列表框中，选择 DMZ 选项，在 Pool ID 文本框中输入新创建地址池的 ID 号，如 1。

（4）在 IP Addresses to Add 区域，指定 DMZ 接口使用的 IP 地址范围。

（5）单击 Add 按钮，将该 IP 地址范围添加至地址池。

（6）单击 OK 按钮，返回至 NAT Rules 窗口。

3．为外部端口指定 IP 地址池

为外部端口指定 IP 地址被用于转换私有 IP 地址，从而实现内部客户端对 Internet 的安全访问。借助 PAT 技术，可以使用同一合法 IP 地址将内部不同的服务器发布至 Internet。

（1）在 NAT Configuration 窗口右侧选择 Global Pools 选项卡，单击 Add 按钮，显示如图 12-29 所示的 Add Global Address Pool 对话框。

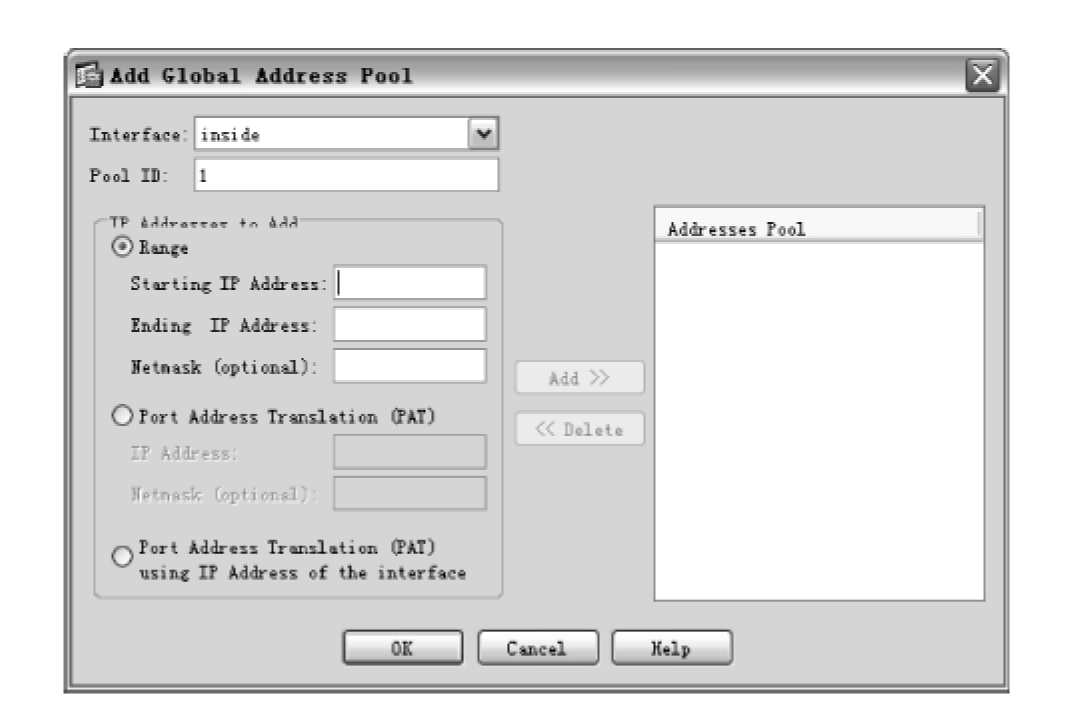


图 12-28　Add Global Address Pool 对话框

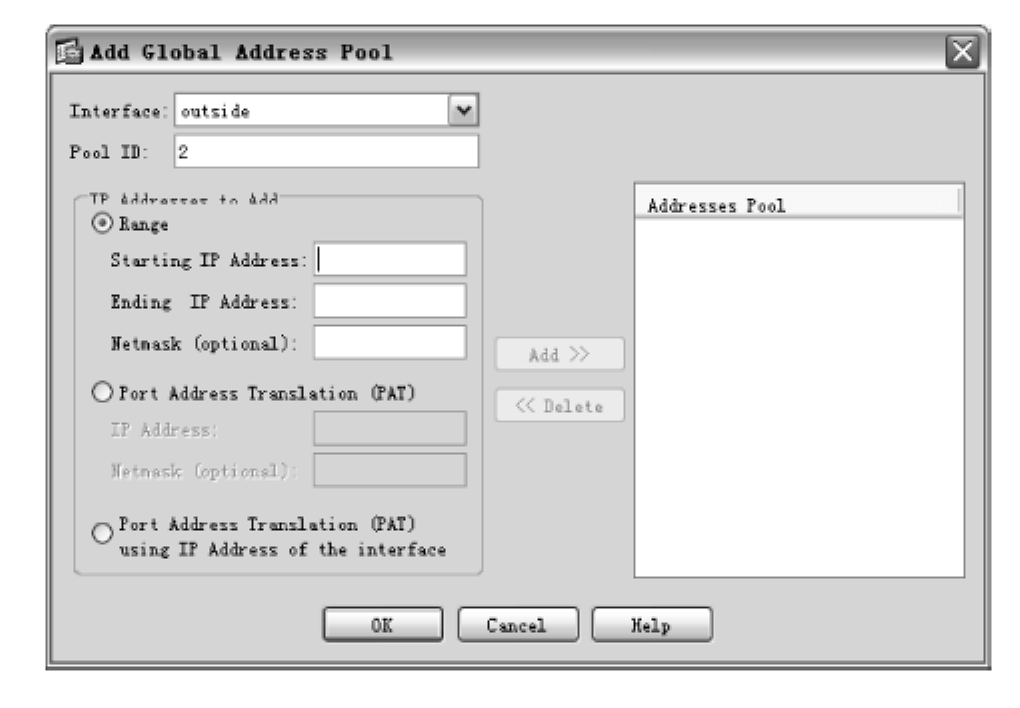


图 12-29　Add Global Address Pool 对话框

（2）在 Interface 下拉列表框中，选择 outside 选项，为外部接口指定地址池 ID 号，例如 2。可以将这些地址添加到与 DMZ 接口相同的 IP 地址池。

（3）选中 Port Address Translation（PAT）using IP Address of the interface 单选按钮，单击 Add 按钮，将该地址添加至 IP 地址池。

（4）单击 OK 按钮，返回 Cisco ASDM 配置窗口。确认配置无误后，在 ASDM 主窗口

中，单击 Apply 按钮即可。

4. 配置内部客户端访问 DMZ 区的 Web 服务器

在上述配置中，为内部客户端设置了安全的私有 IP 地址池，还需要配置一条 NAT 规则，用于实现内部客户端对 DMZ 区域中 Web 服务器的安全访问。

(1) 在 ASDM 主窗口工具栏中，单击 Configuration 图标，在左侧栏中单击 NAT Rules 按钮，显示 NAT Rules 规则对话框。在 Add 下拉列表框中选择 Add Dynamic NAT Rule 选项，显示如图 12-30 所示的 Add Dynamic NAT Rule 对话框。

(2) 在 Real Address 区域，指定被转换的 IP 地址。从 Interface 下拉列表框中，选择 inside 接口，在 IP address 文本框中，输入内部客户端使用的 IP 网络号。

(3) 在 Dynamic Translation 区域，指定转换的目的 IP 地址。从 Interface 下拉列表框中，选择 DMZ 接口，指定该地址池使用动态 NAT 规则。选中 Select 复选框，选择全局地址池 ID。

提示：如果欲添加的地址池不存在，可以单击 Add 按钮创建新的 IP 地址池。

(4) 单击 OK 按钮，添加动态 NAT 规则，并返回至 NAT 窗口。ASDM 将添加两条规则，因为同一 IP 地址池同时被转换使用。

5. 配置内部客户端访问 Internet

在上述配置中，借助 NAT 规则，可以实现内部客户端对 DMZ 区中 Web 服务器的访问。当然，借助 NAT 规则也应当能够实现内部客户端对 Internet 的访问。不过，管理员无须再创建任何规则，因为 IP 地址池包括了两种需要转换的地址，即 DMZ 接口使用的 IP 地址和外部接口使用的 IP 地址。

6. 为 Web 服务器配置外部 ID

DMZ 中的 Web 服务器需要为 Internet 中所有的主机提供访问服务。该配置需要将 DMZ 中的 Web 服务器的私有 IP 地址转换为公有 IP 地址，允许外部 HTTP 客户端实现对 Web 服务的访问。

(1) 在 ASDM 主窗口工具栏中，单击 Configuration 图标。在左侧栏中单击 Firewall 选项中的 NAT Rules 按钮，从 Add 下拉列表框中，选择 Add Static NAT Rule 选项，显示如图 12-31 所示的 Add Static NAT Rule 对话框。

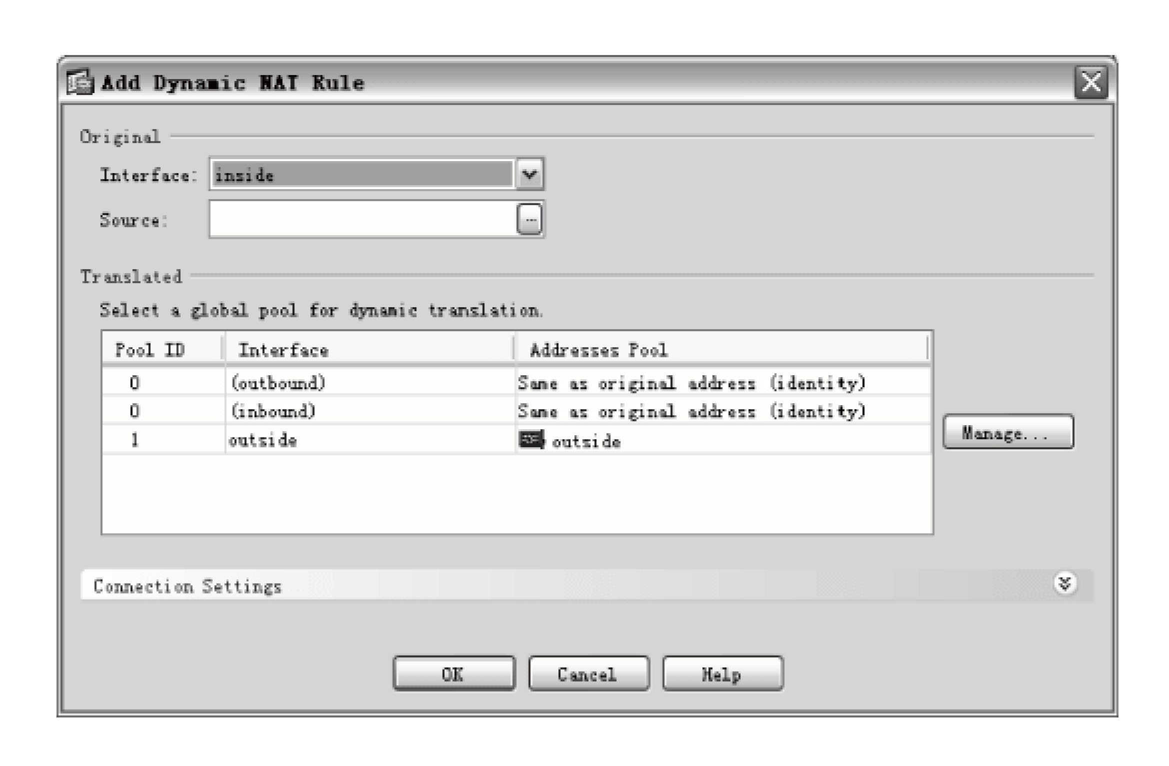


图 12-30 Add Dynamic NAT Rule 对话框

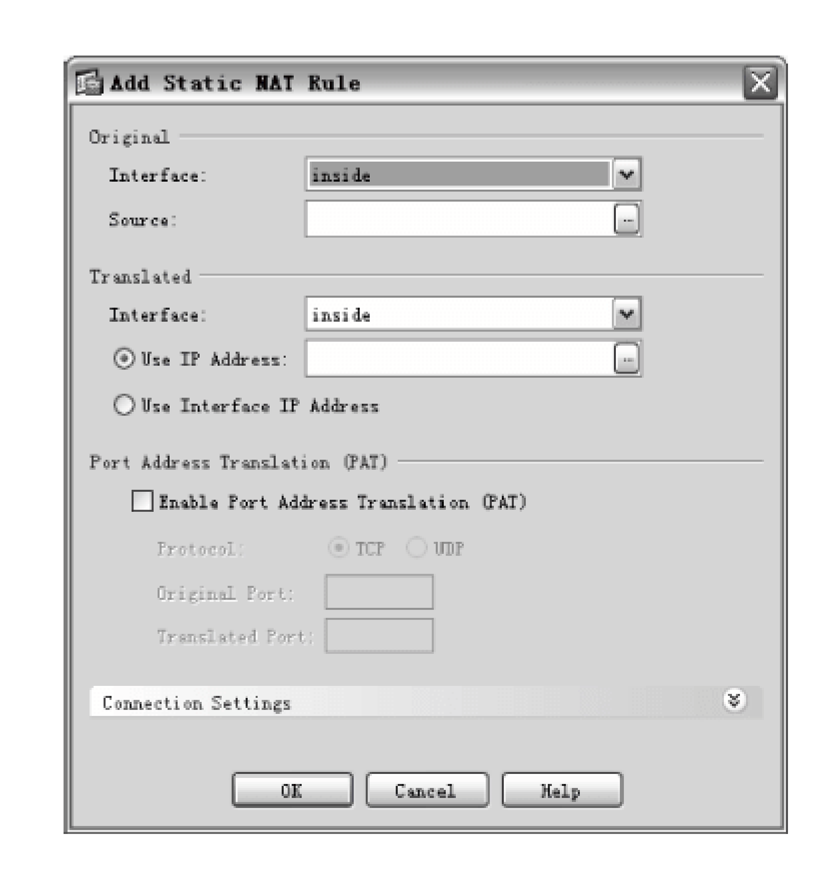


图 12-31 Add Static NAT Rule 对话框

（2）从 Interface 下拉列表框中，选择 DMZ 接口，在 IP Address 文本框中，输入 DMZ 区 Web 服务器的 IP 地址。

（3）在 Static Translation 区域，指定 Web 服务器使用的公有 IP 地址。从 Interface 下拉列表框中，选择 outside 选项，从 IP Address 下拉列表框中，选择 DMZ 区 Web 服务器使用的公有 IP 地址。

（4）单击 OK 按钮，添加规则并返回 Address Translation Rules 列表。

（5）单击 Apply 按钮，保存安全配置的修改。

7. 允许 Internet 用户访问 DMZ 的 Web 服务

默认情况下，安全设备禁止来自公共网络的所有通信。因此，必须创建一个安全规则，允许来自 Internet 用户对 DMZ 区中 Web 服务器的访问，即允许来源于 Internet 任意用户的针对 DMZ 中 Web 服务器的流入和流出的 HTTP 通信。

（1）在 ASDM 主窗口工具栏中，单击 Configuration 图标。在左侧栏中单击 Security Policy 按钮，从 Add 下拉列表框中，选择 Add Access Rule 选项，显示如图 12-32 所示的 Add Access Rule 对话框。

（2）在 Interface 下拉列表框中，选择 outside 选项，在 Action 单选项中，选中 Permit 单选按钮。

（3）在 Source 区域，设置允许发起访问的源 IP 地址，显示如图 12-33 所示的 Browse Source 对话框。

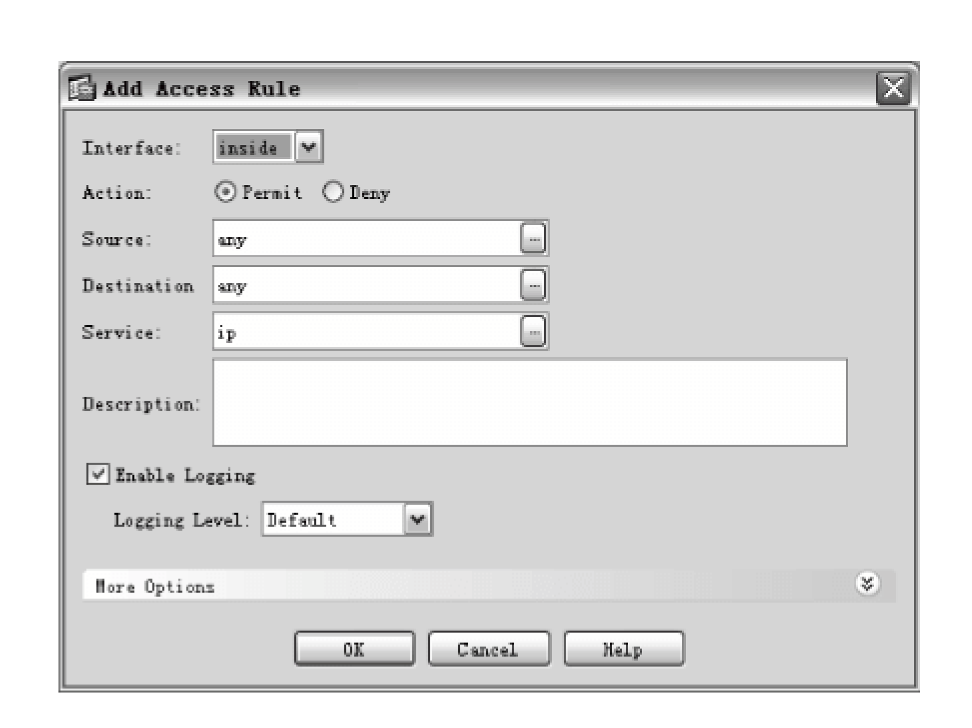


图 12-32　Add Access Rule 对话框

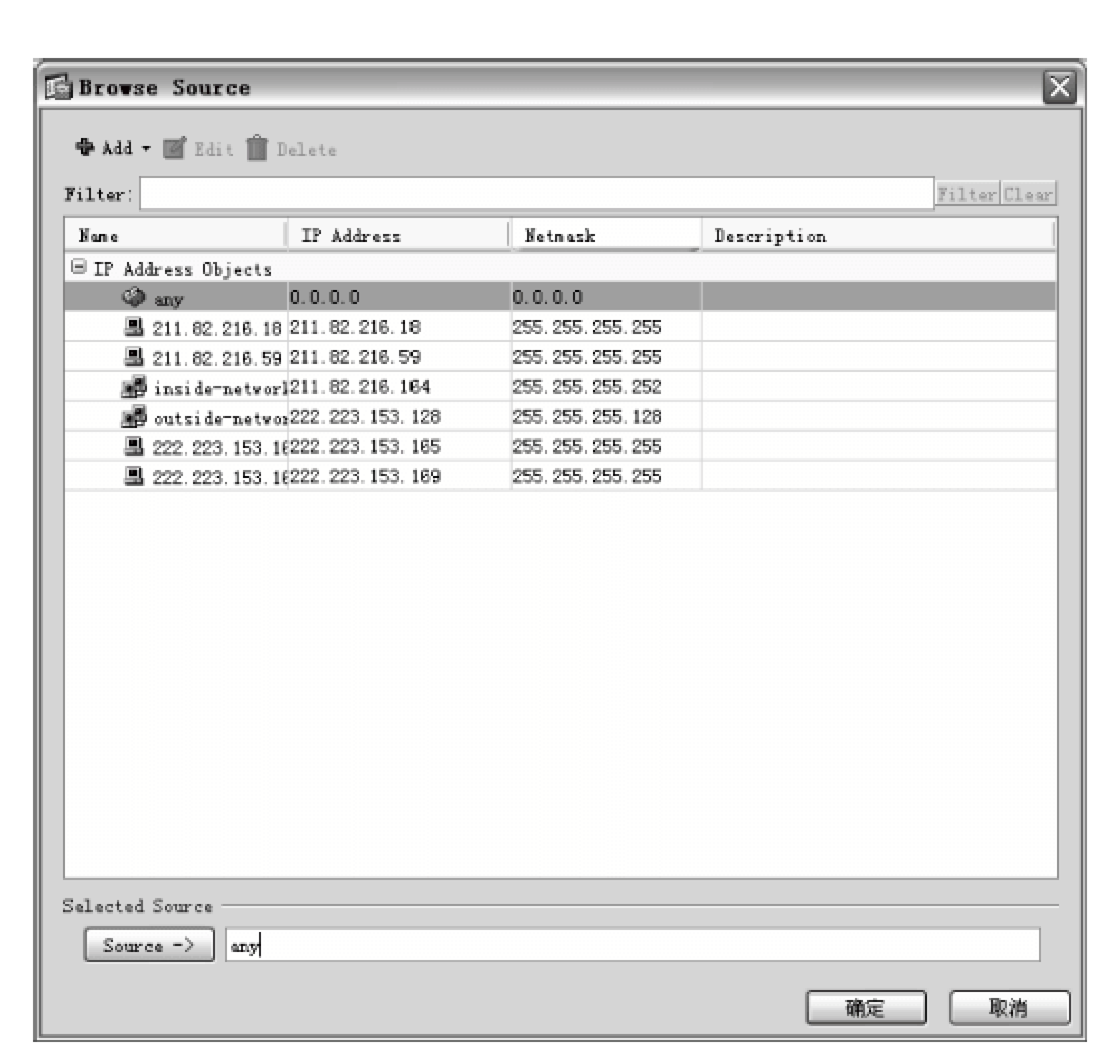


图 12-33　Browse Source 对话框

（4）在 Destination 区域设置允许访问的目的 IP 地址，显示如图 12-34 所示的 Browse Destination 对话框。

（5）在 Service 选项中，指定 IP 地址，显示如图 12-35 所示的 Browse Service 对话框。

（6）在 Description 文本框中，设置 DMZ 描述信息。

（7）单击 More Options 选项，显示如图 12-36 所示的 Add Access Rule 对话框。

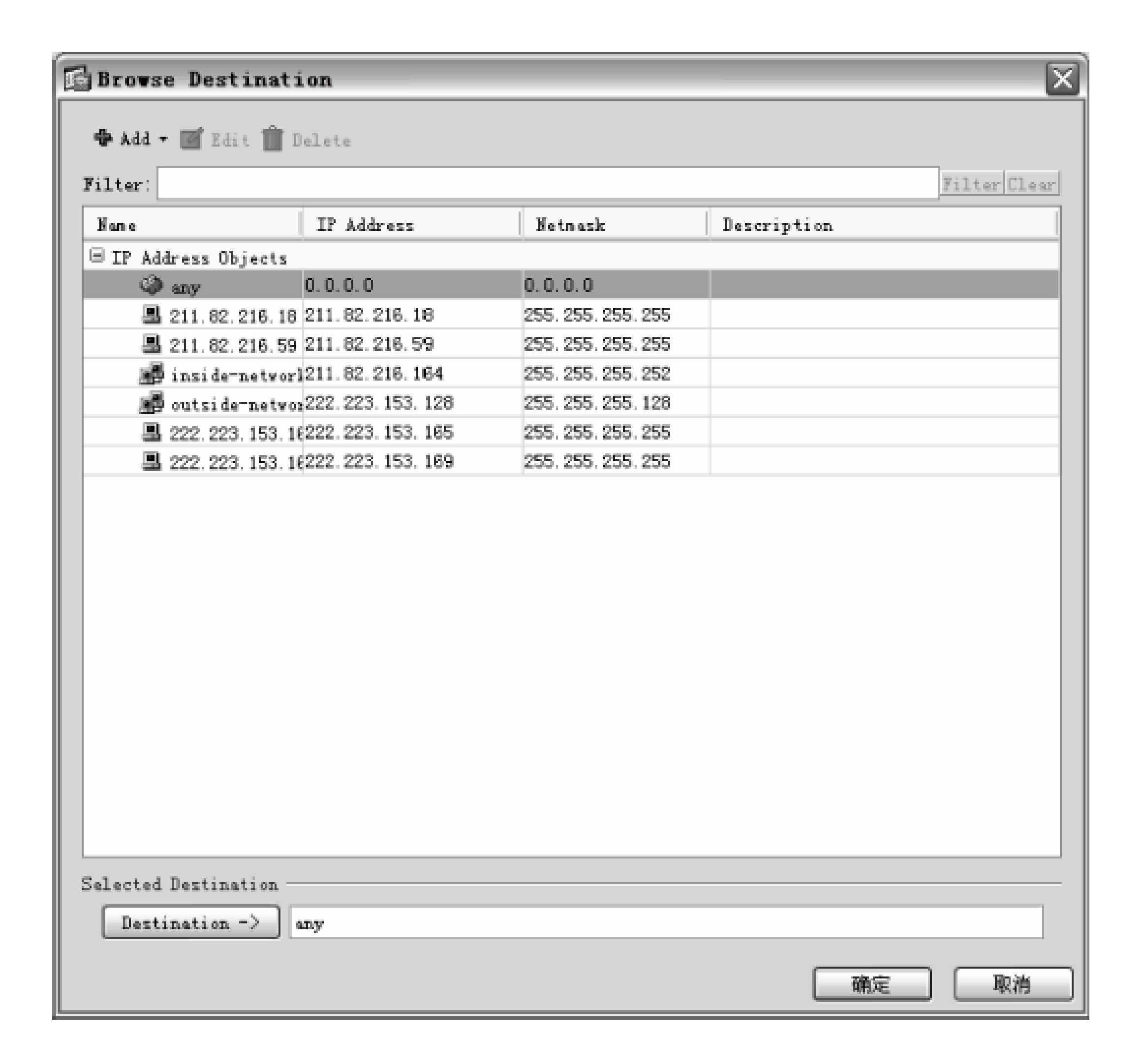
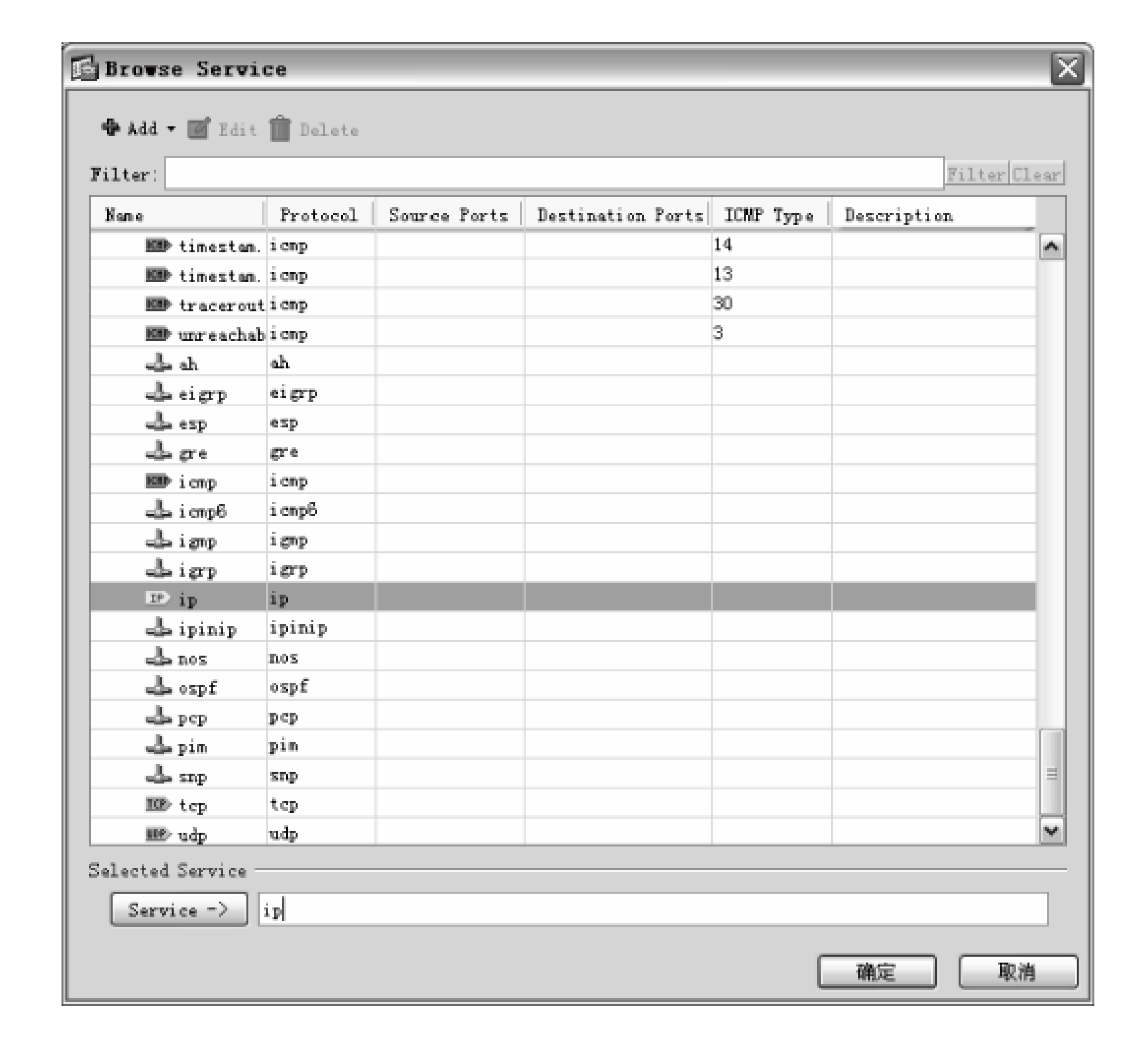


图 12-34 Browse Destination 对话框



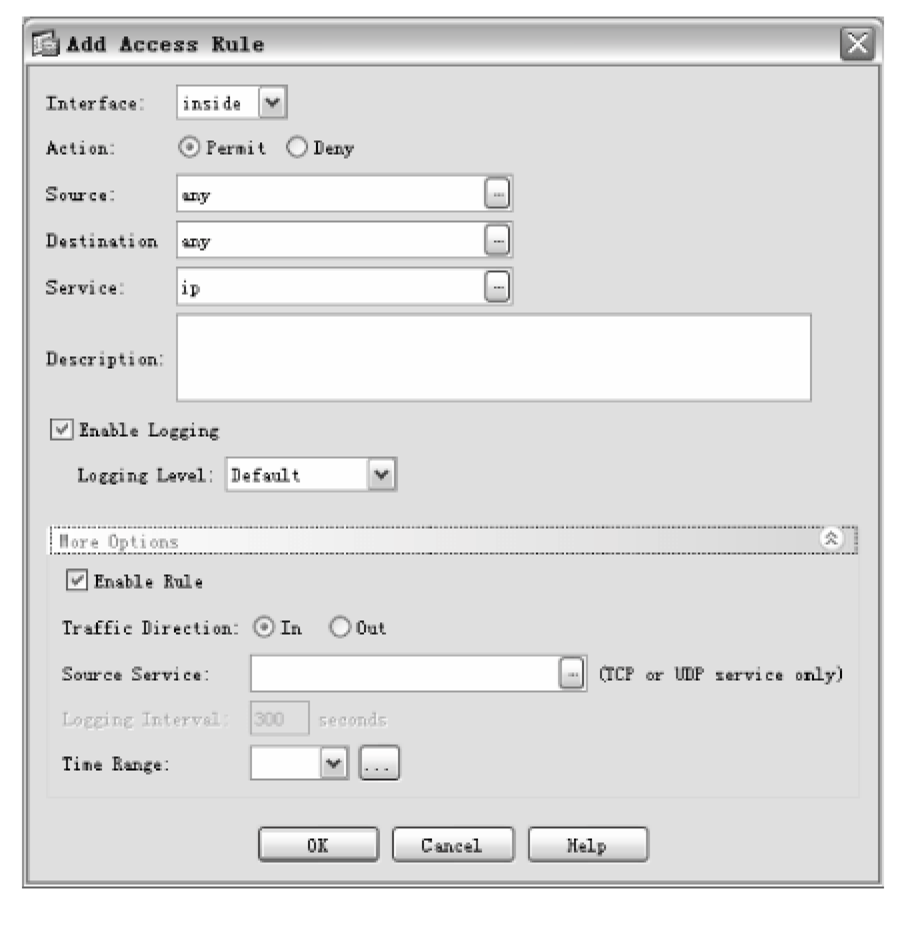


图 12-35 Browse Service 对话框　　　　图 12-36 Add Access Rule 对话框

(8) 单击 Source Service 选项，显示如图 12-37 所示的 Browse Source Service 对话框，添加 TCP 或 UDP 服务。具体内容参见相关内容，这里不再赘述。

(9) 确认无误后，单击 OK 按钮，返回 Cisco ASDM 主页面，确认配置信息是否正确。然后，单击 Apply 按钮保存配置。此时，私有网络和 Internet 中的所有客户端，都将可以访问 DMZ 区中的 Web 服务。

12.3.6 管理安全设备

使用 Cisco 自适应安全设备管理器管理安全设备，可以通过 Web 图形界面监视设备的运行状态、查看和分析网络流量、查看和分析系统日志和安全监控工具，使管理员能够更好

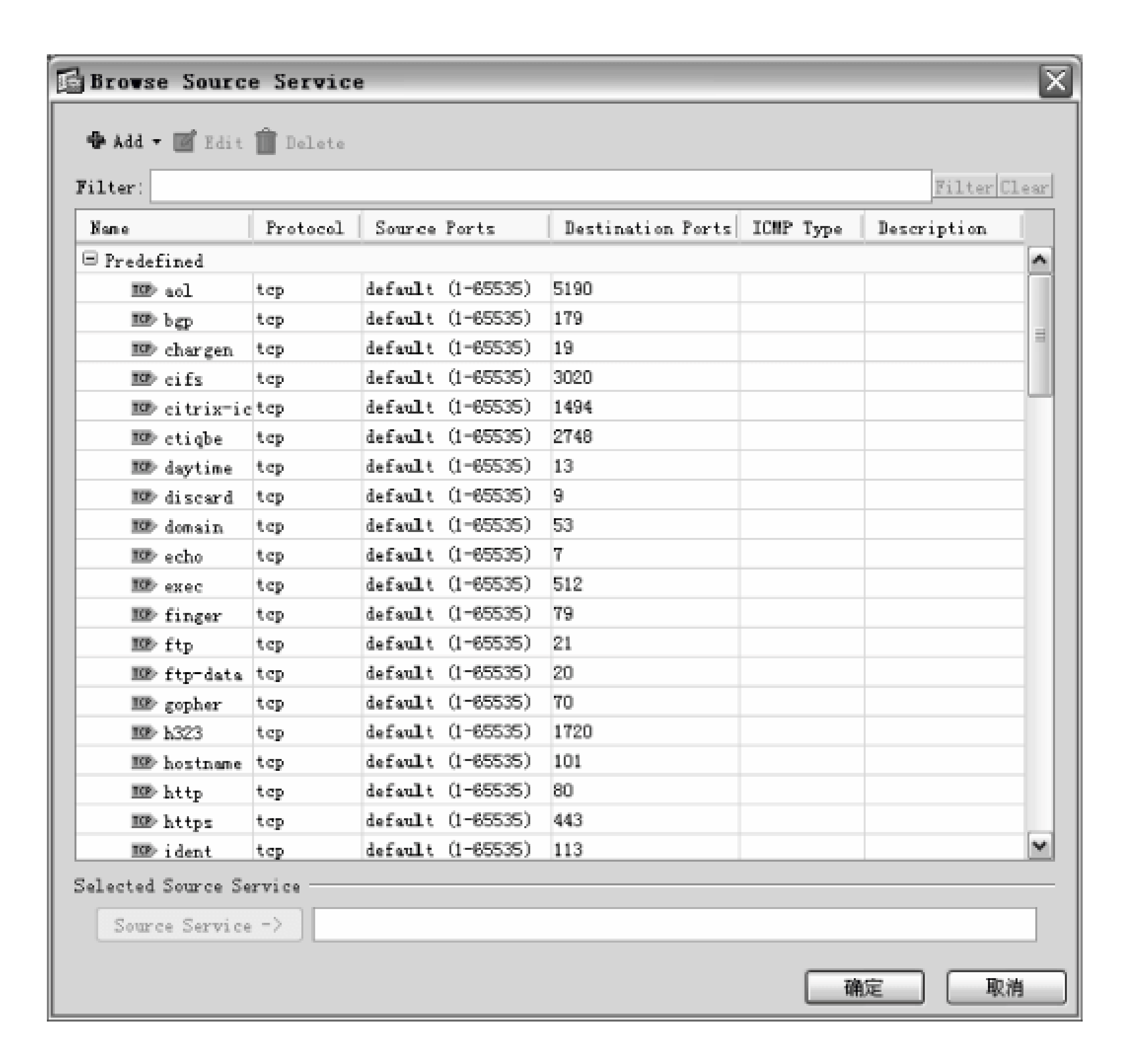


图 12-37　Browse Source Service 对话框

地管理安全设备。

1. 监视安全设备运行状态

利用 Cisco ASDM 登录到 Cisco ASA 主界面(如图 12-38 所示),在 Device Dashboard 选项卡中显示了设备仪表板的信息。显示设备信息(名称、版本、型号等)、系统资源运行状态(CPU 和 Memory)、接口状态和信息传输状态。

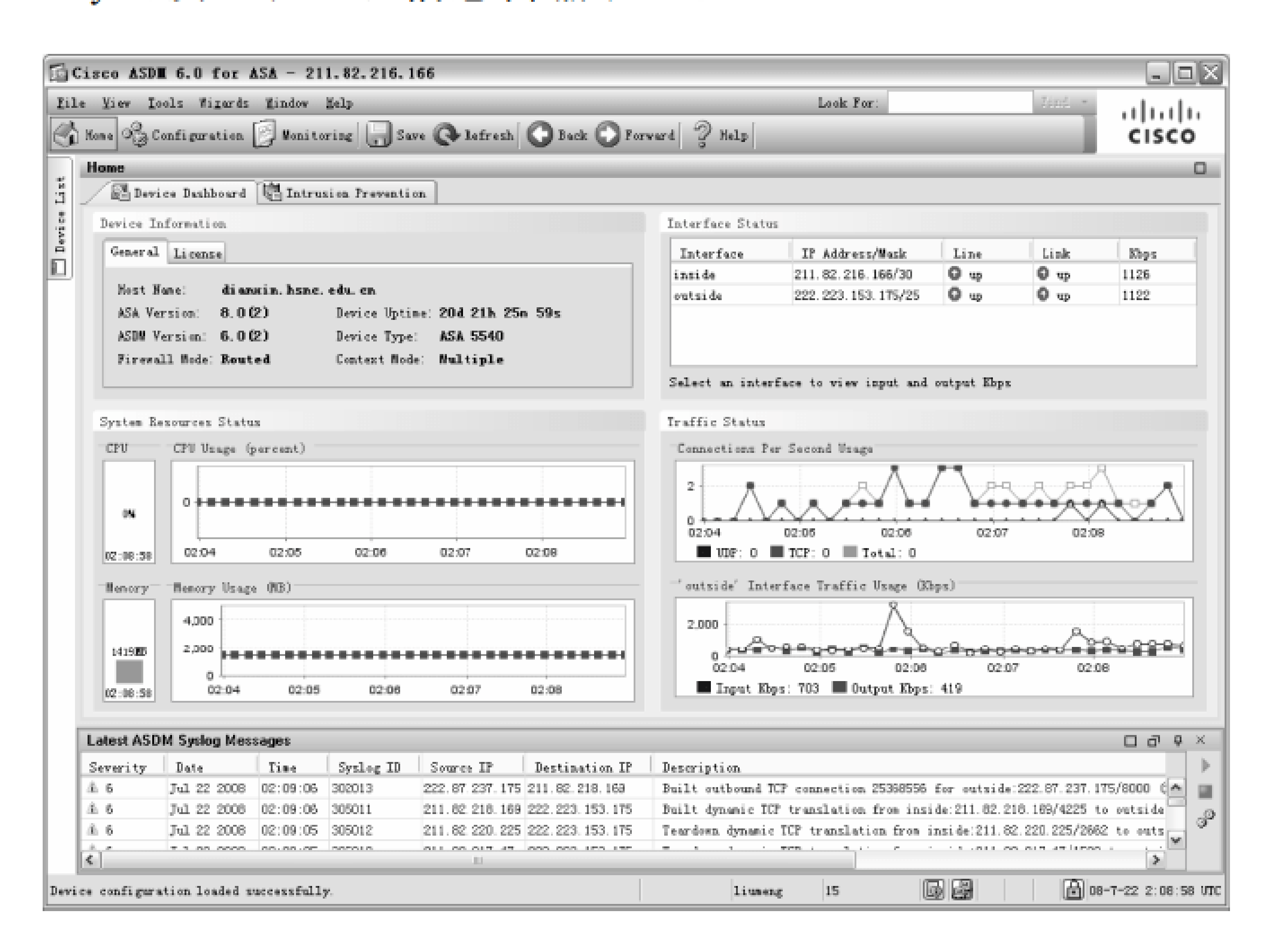


图 12-38　Cisco ASA 主界面

2. 查看和分析网络流量

(1) 在 Cisco ASA 主界面中,单击 Monitoring 按钮,监视设备的接口信息,如图 12-39 所示。

(2) 在左侧 Interfaces 列表栏中选择 Interfaces Graphs 选项,可以查看内部或外部的接口图表,如图 12-40 所示。

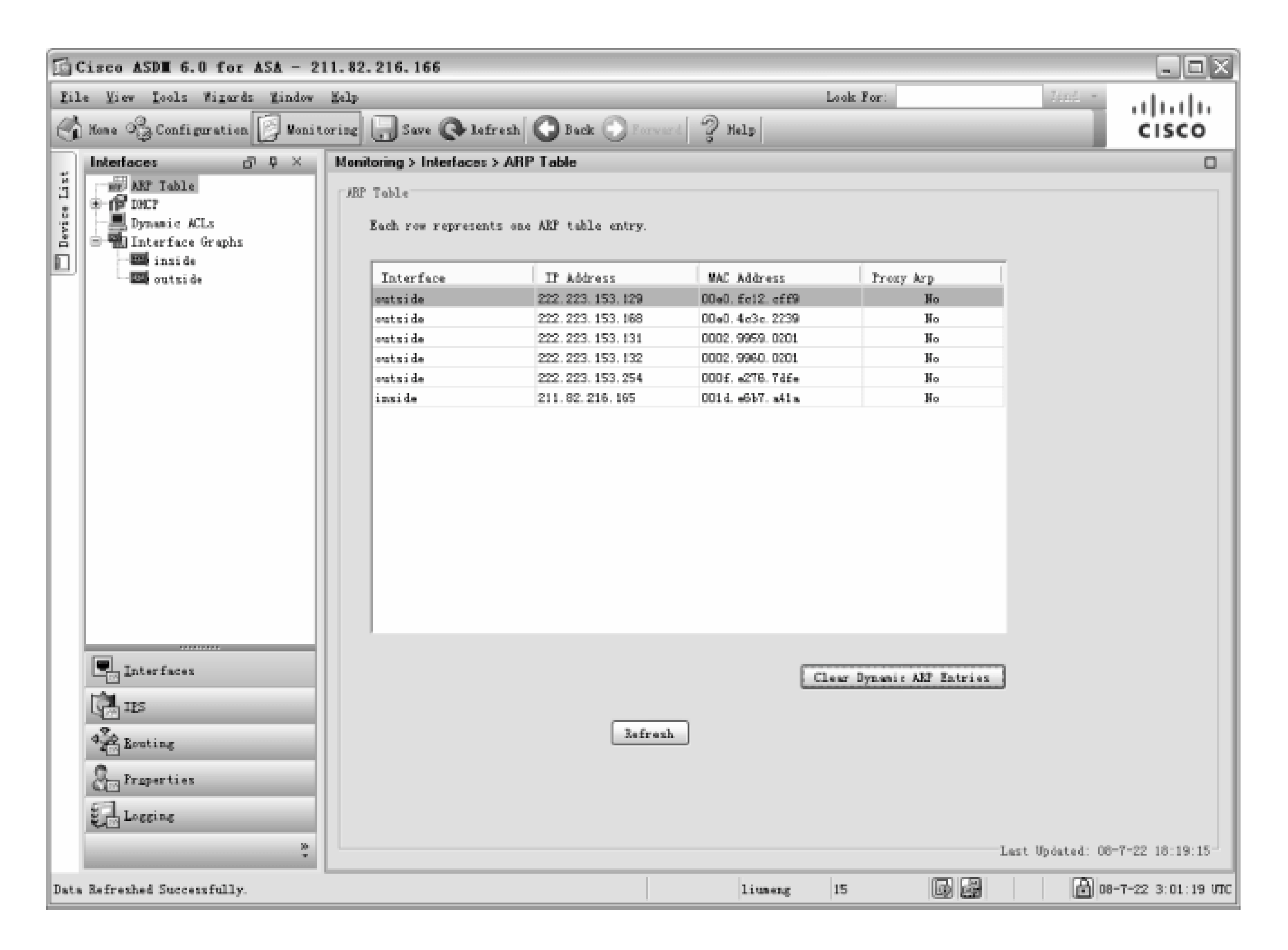


图 12-39　监视设备的接口信息

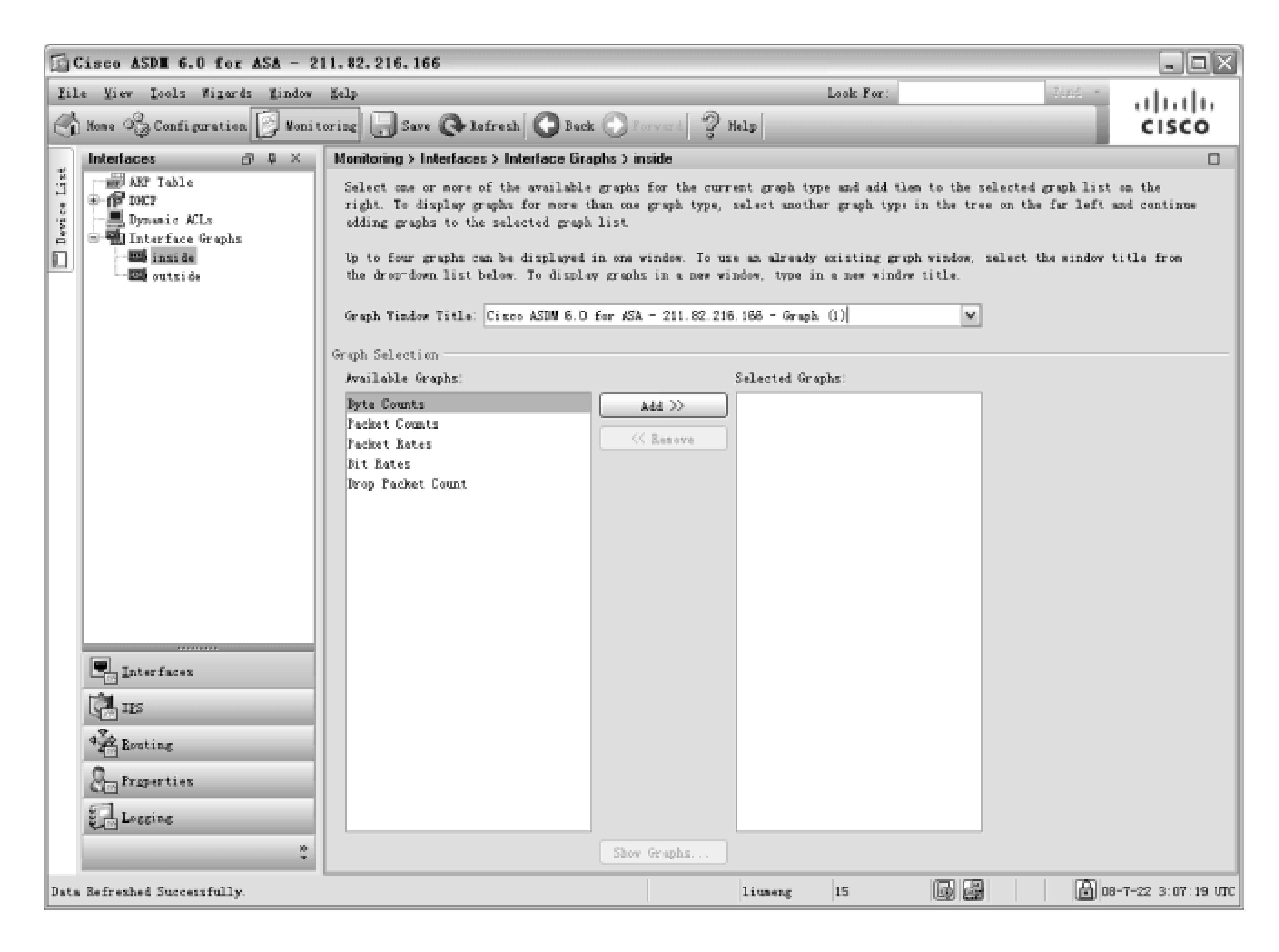


图 12-40　Interfaces Graphs 对话框

(3) 以 inside 为例，在 Graph Selection 对话框中显示图形所选内容，在 Available Graphs 列表框中，选择可用图形并添加到选定的图形 Selected Graphs 列表框中，如图 12-41 所示。

(4) 单击 Show Graphs 按钮，以图例形式显示网络的流量，如图 12-42 所示。

3. 查看和分析系统日志

(1) Cisco ASA 主页左侧栏中，单击 Logging 选项，显示如图 12-43 所示的 Real-Time Log Viewer 对话框，在 Logging Level 列表框中，选择日志记录级别。在 Buffer Limit 文本框中，输入缓冲区限制，一般为默认值即可。

(2) 单击 View 按钮，系统日志以视图方式显示，如图 12-44 所示。

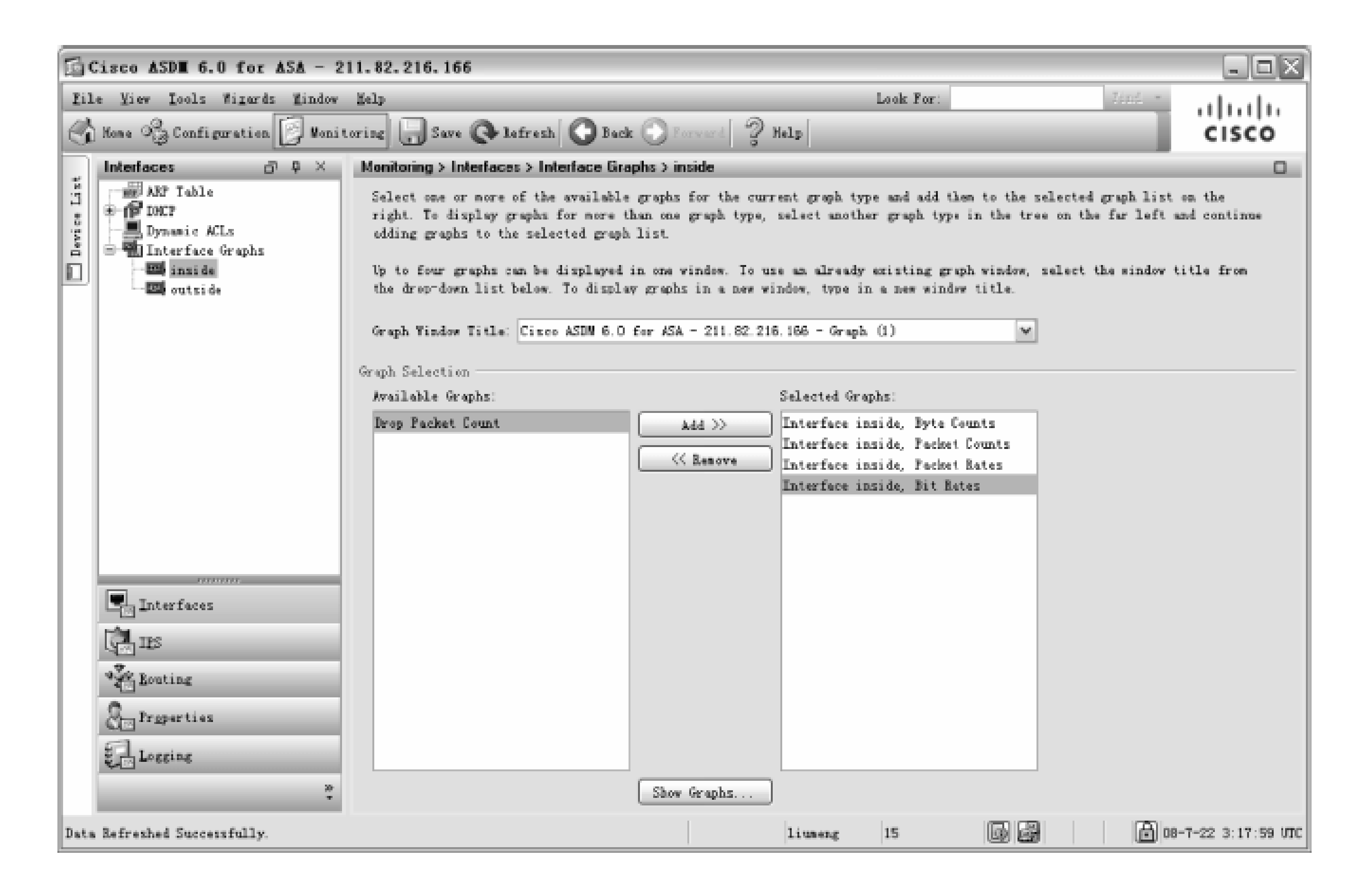


图 12-41　Graph Selection 对话框

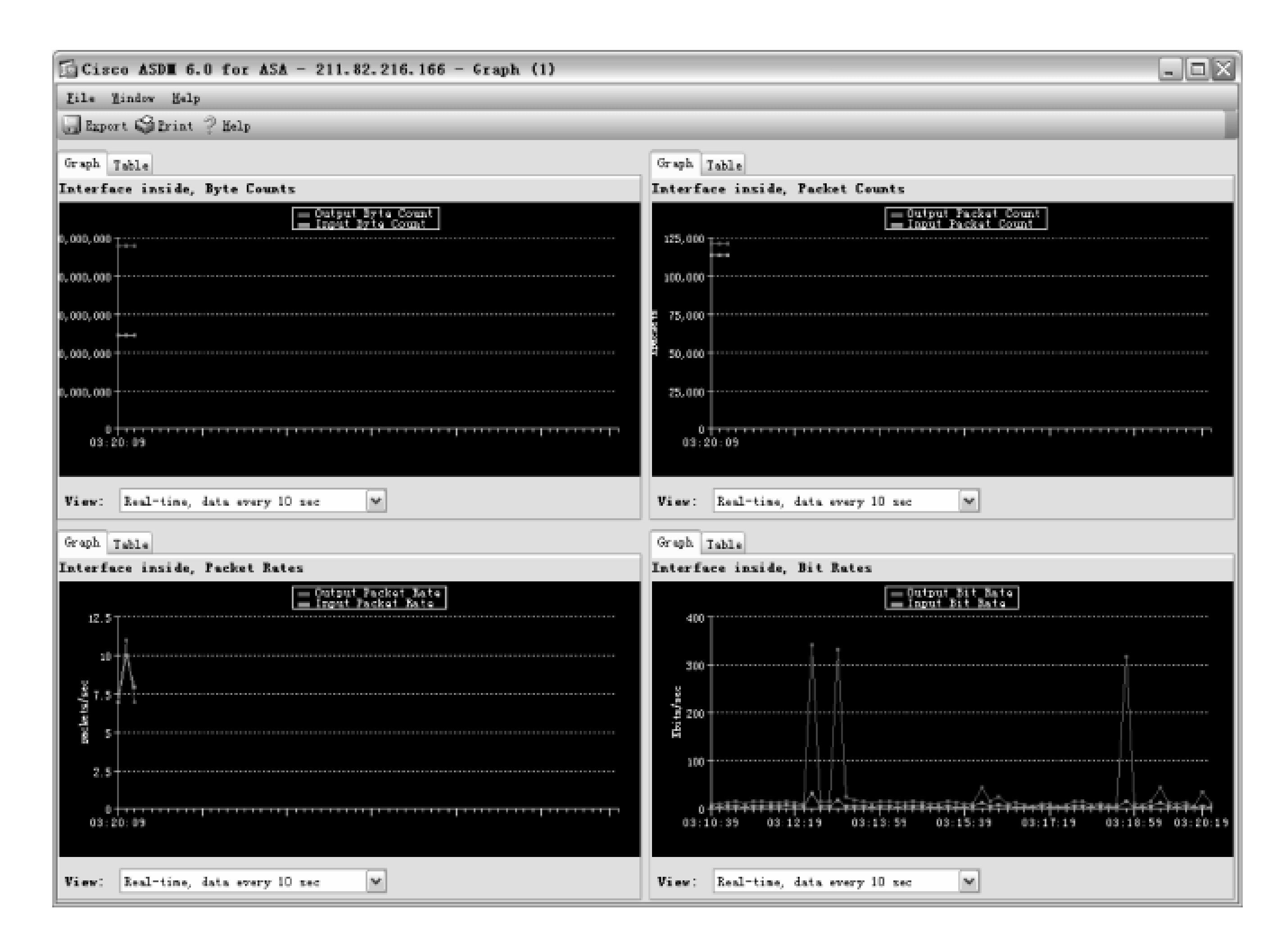


图 12-42　网络流量

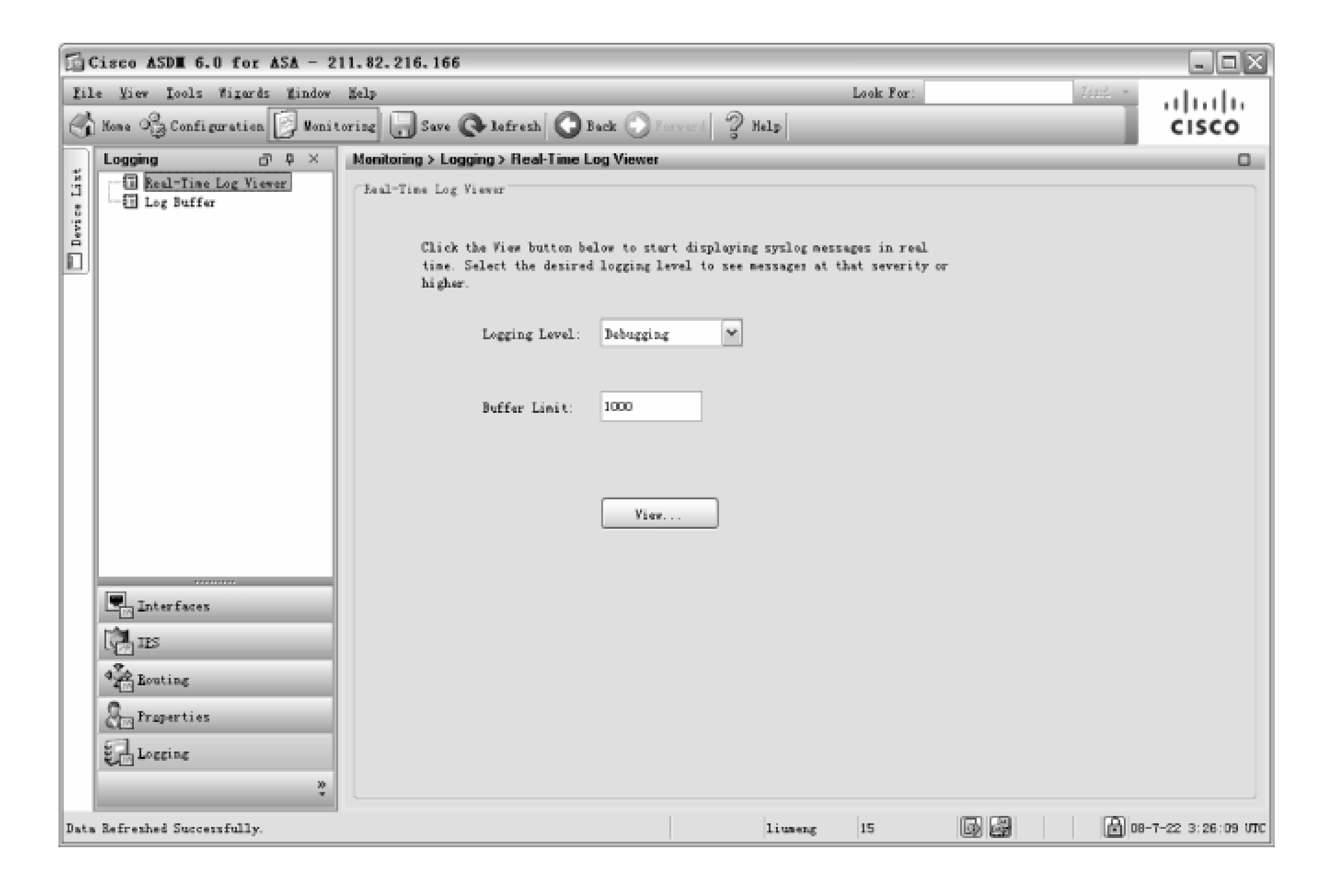


图 12-43　Real-Time Log Viewer 对话框

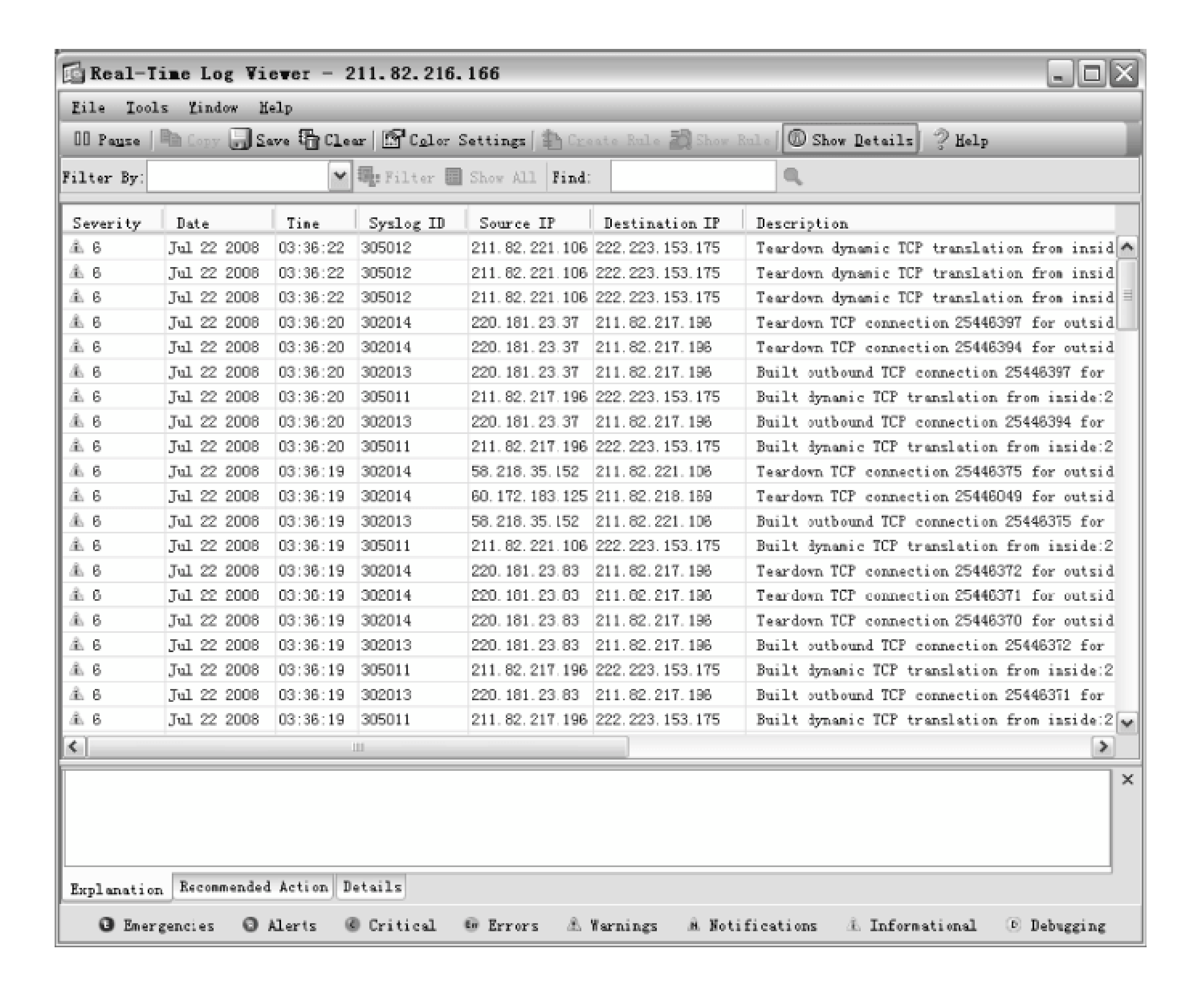


图 12-44　系统日志

4. 安全监控工具

Cisco ASDM 提供了大量监控和报告工具，从而使得安全设备的监控和管理变得更加直观和简单。

(1) 监控工具

Cisco ASDM 6.0 提供了深入的监控和报告服务，以及概览监控功能（如图 12-45 所示）。灵活的分析工具能够创建图形化总结报告，显示了实时使用率、安全事件和网络活动。每个图形化报告中的数据都能以定制增量的形式提供，用户可选择 10s 快照或更长时间间隔的分析。同时，浏览多个图的能力使用户可并行执行具体评估。各图形能方便地标记，并输出数据以便查看。

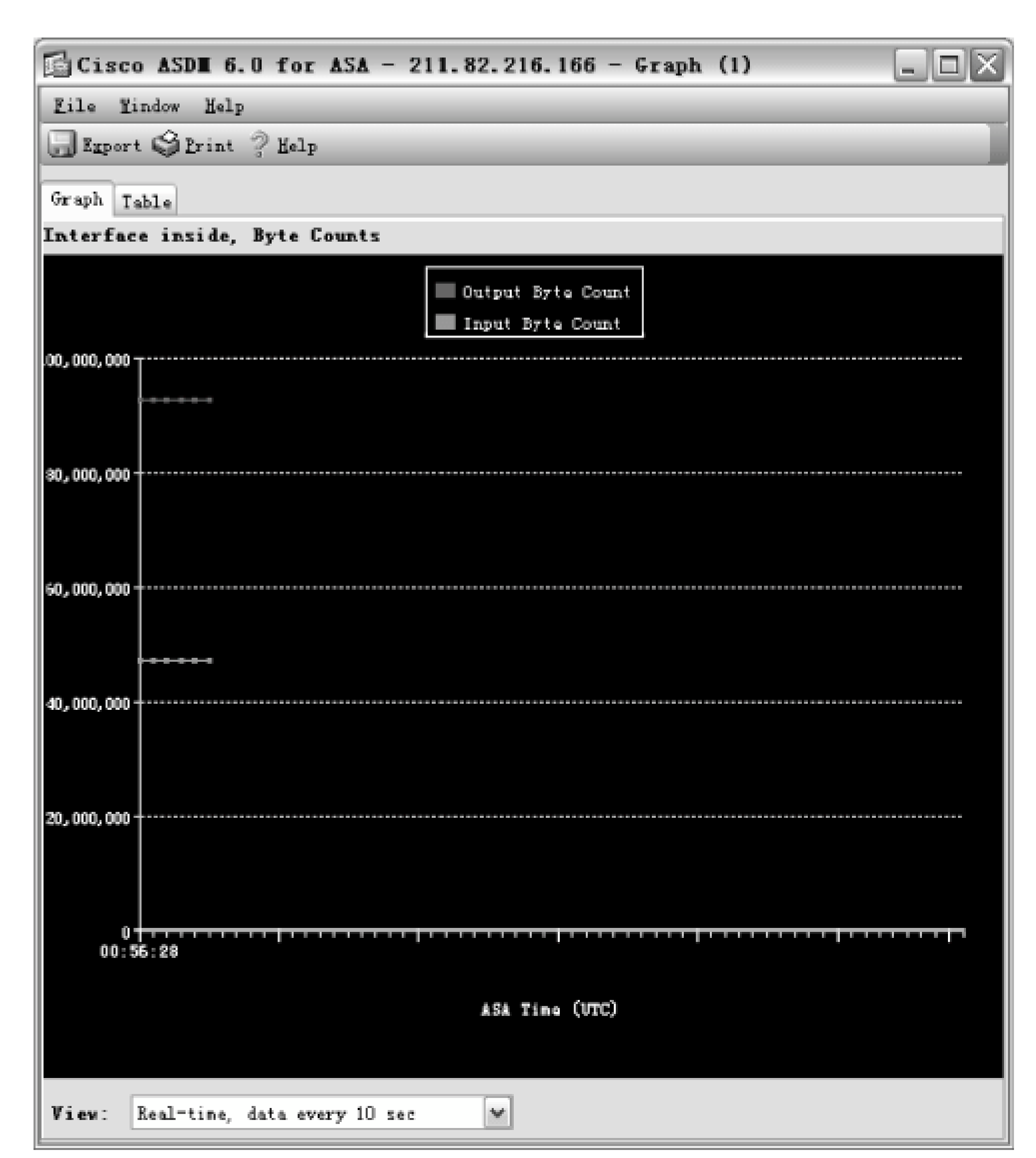


图 12-45　监控窗口

(2) 系统图

提供 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备的具体状态信息，包括所用区块和空闲区块、当前内存利用率和 CPU 利用率。

(3) 连接图

在每秒基础上，跟踪实时进程和连接性能监控数据、地址转换、验证、授权和记账（AAA）事务处理、URL 过滤请求等。连接图使管理员可全面了解其网络连接和活动，且不会被过多信息所淹没。

（4）攻击保护系统图

由16种不同的图形来显示潜在的恶意活动，例如，攻击特征信息显示IP、互联网控制信息协议（ICMP）、用户数据包协议（UDP）、TCP攻击和Portmap请求等活动。这些图形详细显示了攻击者列表、事件列表、系统统计数据和对于Cisco AIP-SSM的诊断。

（5）接口图

提供对安全设备上每个接口的带宽使用率的实时监控。显示内外通信的带宽使用率。用户可浏览分组速率、数目和错误，以及位、字节和冲突数等。

（6）VPN统计和连接图

通过支持Cisco IPSec流量监控MIB，提供对VPN连接的全面显示，每个隧道的具体统计数据，包括隧道正常运行时间和所传输的字节/分组数。

习题

1. 企业网络中常用的安全设备有哪些？主要应用在网络中的哪些位置？
2. 简述IPS的主要功能。
3. 简述Cisco ASA系列产品的功能特点。
4. 什么是DMZ？如何通过Cisco ASA防火墙配置DMZ？

实验：设计安全企业网络

实验目的：

掌握常用安全网络设备的部署与应用。

实验内容：

设计一个简单的企业网络，分别将网络防火墙、IPS、IDS等设备应用到网络中的不同位置。

实验步骤：

（1）设计网络环境，绘制简单的网络拓扑图。

（2）按照网络拓扑图连接网络设备。

（3）为网络设备分配IP地址，并通过客户端测试彼此之间的连通性。

（4）通过客户端观察网络设备的运行状况。

（5）调阅网络设备运行日志并进行分析。

第 13 章 chapter 13

配置网络可靠性

可靠性是衡量网络安全性的重要指标之一，网络的可靠性则主要通过网卡和网络设备的冗余实现，当网卡或网络设备出现故障时，自动启用冗余设备，以保证网络服务的正常提供。此外，冗余网卡或设备还可以起到负载平衡的作用，当设备处于超负荷工作状态时，冗余设备可以自动分配相应的负载，从而提高网络传输速率和效率。

13.1 网络可靠性规划

可靠性是网络规划设计与性能评价的重要指标。计算机网络的可靠性一般包括网络的生存性、抗毁性及有效性等多个方面，涉及网络通信设备、拓扑结构、通信协议等多方面因素。实际应用中，应根据计算机网络的主要功能应用，做好关键环节的设备冗余和数据备份，从而确保网络的可靠性和稳定性。

13.1.1 案例情景

该企业网络属中小型企业网络，一般情况下对网络可靠性要求并不高，随着企业的发展，网络可靠性的重要程度日益显现。办公区网络不仅要求随时连接到主干网络，访问企业内部的服务器资源，而且需要实时连接到 Internet。

随着计算机网络应用的不断深入，企业之间的交流，企业内部部门之间的交流，都是通过视频会议系统实现的。视频会议系统对网络连接的可靠性要求是非常高的，短暂的网络连接中断，可能会给企业造成无法估计的损失。

13.1.2 项目需求

企业网络的可靠性保障措施首先要保证内部网络连接的可靠性，重要部门在访问网络中心服务器时能实现路由冗余和负载均衡，跨越交换机的关键子网之间互访时也应可以实现路由冗余，从而保证企业内关键业务的不间断运行。

13.1.3 解决方案

用户可以通过容错和冗余的方法提高网络的可靠性，一般包括如下方面。

(1) 软件容错。以软件为主的容错系统一般由两套设备构成，其中一台作为主机；另一台作为备份机。当主机出现故障时，马上将工作转到备份机。例如基于 Windows 系统的

负载均衡技术。

(2) 硬件容错。硬件容错主要是采取冗余技术,用加大投资和降低速度的代价来换取可靠性。可作冗余设计的设备很多,从 CPU、网卡、磁盘控制器到磁盘存储器,都可以采用多套设备并存的方式,用多数表决技术或两两比较技术进行容错。

(3) 数据备份。数据备份是每一计算机网络管理员都要定期进行的工作,所谓数据备份就是将数据从服务器的硬盘中复制到可移动介质上(如磁带、大容量软盘或光盘上)并将其保存到更安全的场所的过程。

1. 软件容错

所谓软件容错,就是指通过软件实现网络应用的冗余或容错,例如,基于 Windows 系统实现的群集、负载均衡等技术都属于软件容错的范畴。

(1) 群集

群集技术就是将某一项重要的网络应用分担到不同的服务器上,从而降低每一台服务器的工作强度,达到提高可靠性的目的。群集技术可以使用户免于整个系统的瘫痪以及操作系统和应用层次的故障。一台服务器集群包含多台拥有共享数据存储空间的服务器,各服务器之间通过内部局域网进行互相连接;当其中一台服务器发生故障时,它所运行的应用程序将与之相连的服务器自动接管;在大多数情况下,集群中所有的计算机都拥有一个共同的名称,集群系统内任意一台服务器都可被所有的网络用户所使用。

(2) 负载均衡

负载均衡(Load Balance)是建立在现有网络基础结构上的,它提供了一种廉价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

负载均衡有两方面的含义。首先,大量的并发访问或数据流量分担到多台节点设备上分别处理,减少用户等待响应的时间;其次,单个重负载的运算分担到多台节点设备上做并行处理,每个节点设备处理结束后,将结果汇总,返回给用户,系统处理能力得到大幅度提高。

2. 硬件容错

网络可靠性的一个重要的组成部分就是网络设备的可靠性问题,网络设备的可靠性主要通过设备冗余和功能模块冗余来实现。

(1) 交换机的可靠性

交换机是网络中的交换核心,对网络可靠性有很大的影响。因此,在选用交换机时要注意如下问题。

① 交换机应具有较强的微分段能力,可以灵活地将网络划分成较小的冲突域,并在各网段之间起到隔离的作用,以提高整个系统的带宽和性能。

② 交换机应具有很强的容错特性,例如带电插拔、电源备份、电源负载自动平分、链路容错、引擎备份等;此外,交换机还应提供先进的网络诊断工具,实现对交换机的管理和错误诊断。

③ 交换机应具有支持构建虚拟网的能力。虚拟网技术可以大大增加网络的灵活性和智能性,改善网络的性能和可管理性。

(2) 路由器的可靠性

路由器主要是通过路由协议工作的,复杂的路由协议会过多消耗路由器的硬件资源,从

而影响网络的可靠性。为确保路由器的可靠性,首先应删除不支持和不必要的路由协议,建立一致的局域网和广域网协议。其次,在条件允许的情况下应考虑启用路由冗余技术,即在企业网络的同一位置(如网络出口)部署两台完全系统的路由器。这两个路由器保持相同的配置;连接在相同网络上的端口分配相同的IP地址。当主路由器正常工作时,由于次路由器具有相同的路由表和IP地址,因此不会影响网络正常运行;若主路由器出现故障,次路由器立即能自动代替其工作。

3. 数据备份

数据是网络应用的根本。对于一个安全性要求较高的企业网络而言,数据备份应该是网络管理员每天必须完成的任务。备份数据的目的就是为了应对不时之需,一旦存储设备故障或数据遭到破坏,可以立即应用备份及时恢复,将损失减到最小。数据备份的目标主要包括域控制器、邮件服务器、企业网站等。

通常情况下,Windows系统集成的备份工具就可以帮助管理员完成大部分数据的备份工作,必要时用户也可以选择第三方工具实现数据备份和恢复。

13.2 服务器容错

网络服务器是计算机网络的核心设备。容错系统是服务器领域的重要技术之一。容错系统一般有两种,即因有热备份方案而允许出错的系统,和对出错非常敏感的系统。企业网络中关键部门的服务器是不允许停机的,即使是在计划内系统管理和维护时也不例外。服务器容错技术的出现保证了业务系统7×24小时不间断运转,极大地降低了企业业务在各种不可预料灾难发生时的损失。

13.2.1 配置故障转移群集

故障转移群集是Windows Server 2008系统为用户提供的一种技术手段,用户可以根据实际网络需求实现各种类型的Windows群集,例如DFS群集、DNS群集、DHCP群集等。此处以DHCP服务器群集为例介绍故障转移群集的配置和应用。

1. 准备工作

故障转移群集必须满足硬件、软件和网络基础结构的某些要求,并且它需要一个具有适当域权限的管理员账户。

(1) 服务器:建议使用一组包含相同或相似组件的匹配计算机。

(2) 网卡及连接:网卡必须能够被系统识别且通过相关认证。如果使用iSCSI,则应将网络适配器专用于网络通信或iSCSI,而不能同时用于两者。

(3) 系统需求:故障转移群集中的所有服务器必须全部运行Windows Server 2008系统的同一版本,即单个故障转移群集内的节点不能运行不同的版本。另外,所有服务器应具有相同的软件更新和Service Pack。

2. 安装"DHCP服务器"角色服务

群集设置完成后,每台节点服务器中添加"DHCP服务器"角色,在"添加角色向导"安装的过程中,不要设置DHCP作用域,如图13-1所示。具体安装"DHCP服务器"角色服务的具体操作,参见相关内容,这里就不再赘述。

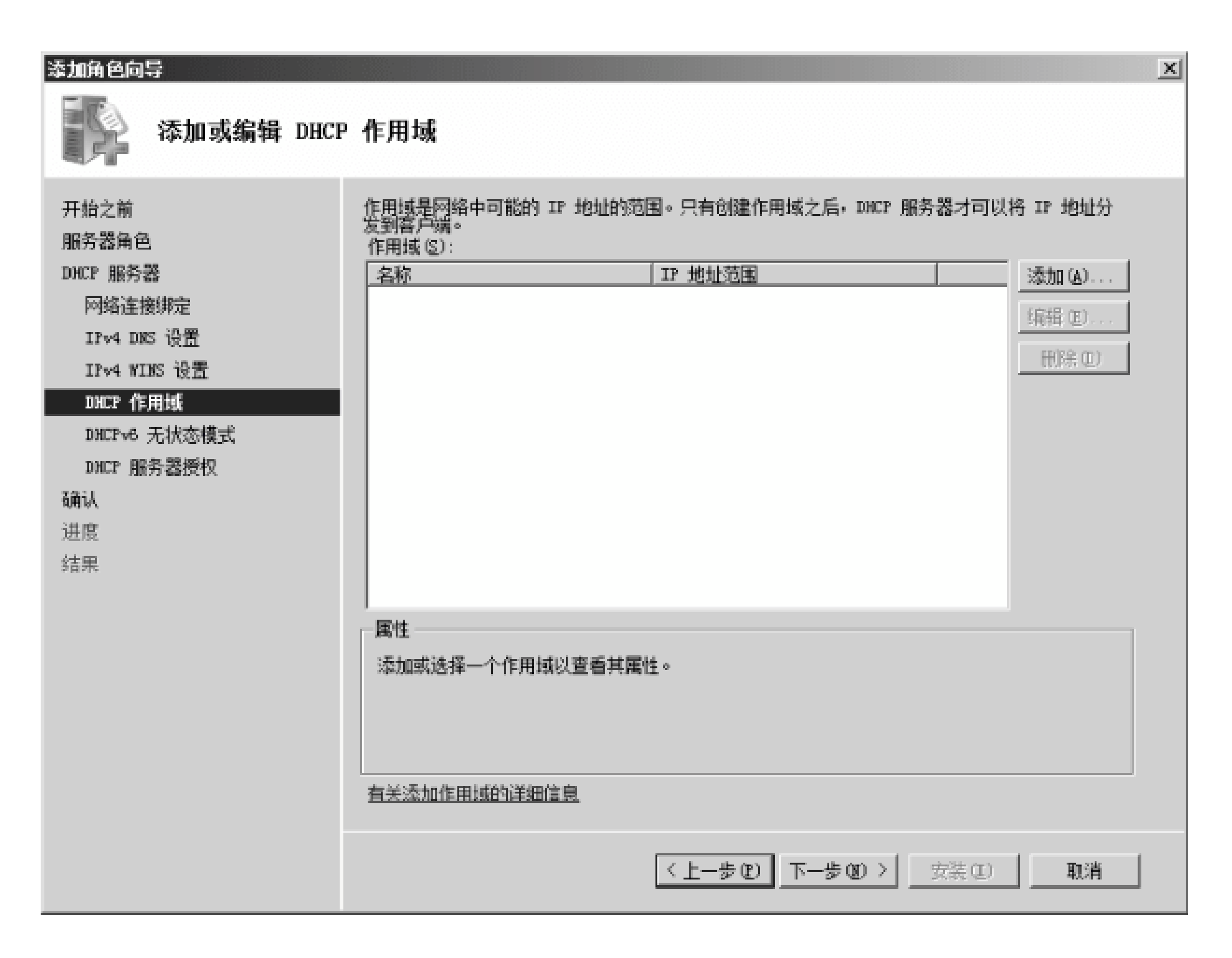


图 13-1 “添加或编辑 DHCP 作用域”对话框

3. 配置 DHCP 服务器群集

Windows Server 2008 的故障转移群集中，应用程序群集是通过使用“高可用性向导”来完成的。另外，在配置 DHCP 服务器群集前，应为该 DHCP 服务器群集规划一个静态的 IP 地址和 DHCP 服务器群集名称。

(1) 在“故障转移群集管理”窗口中，右击“服务和应用程序”并在快捷菜单中选择“配置服务或应用程序”选项，显示如图 13-2 所示的“开始之前”对话框。

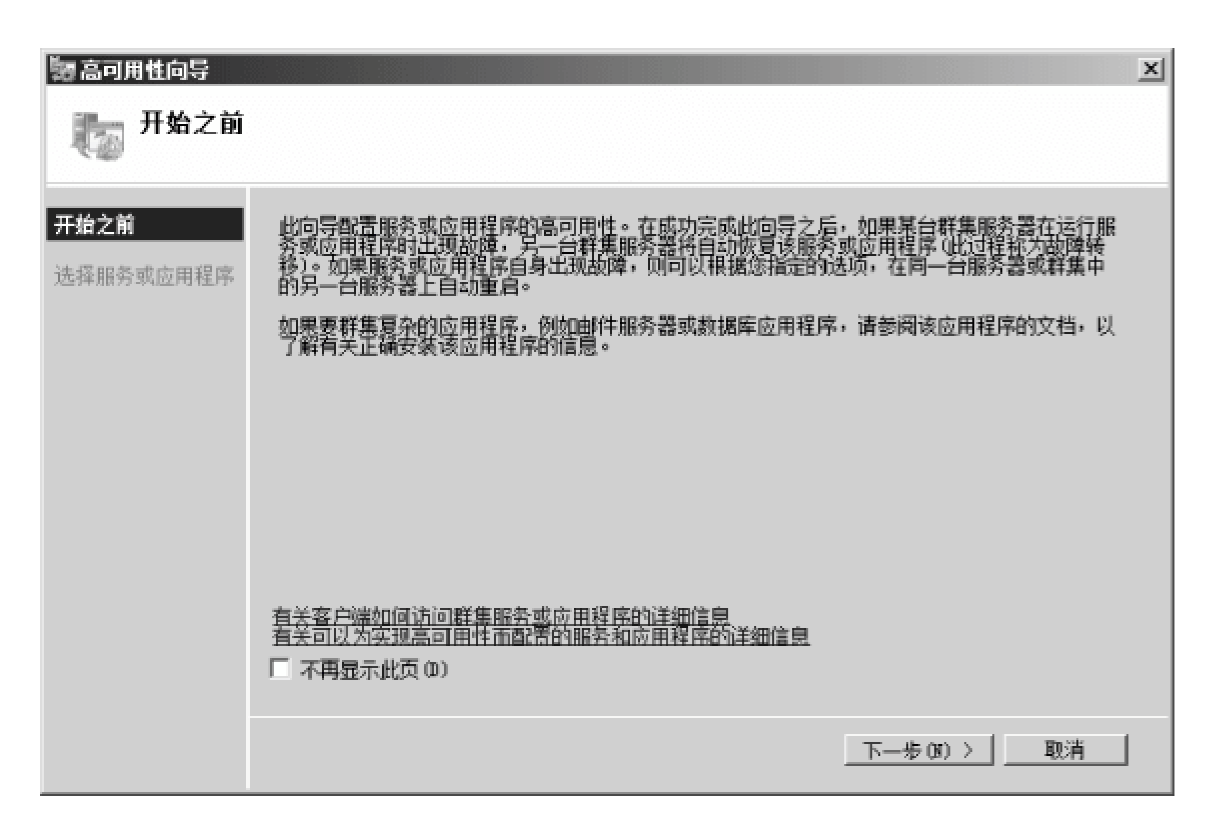


图 13-2 “开始之前”对话框

(2) 单击“下一步”按钮，显示如图 13-3 所示的“选择服务或应用程序”对话框。在“选择要配置为高可用性的服务或应用程序”列表中，选择“DHCP 服务器”选项。需要注意的是，当选中“DHCP 服务器”选项，“下一步”按钮并不会立即显示为可用状态，此时向导会检查故障转移群集的相关配置，当检查通过后该按钮才会显示为可用状态。

(3) 单击“下一步”按钮，显示如图 13-4 所示的“客户端访问点”对话框。在“名称”文本框中，输入 DHCP 服务器名称。在“地址”文本框中，输入客户端用户访问的服务器 IP 地址。

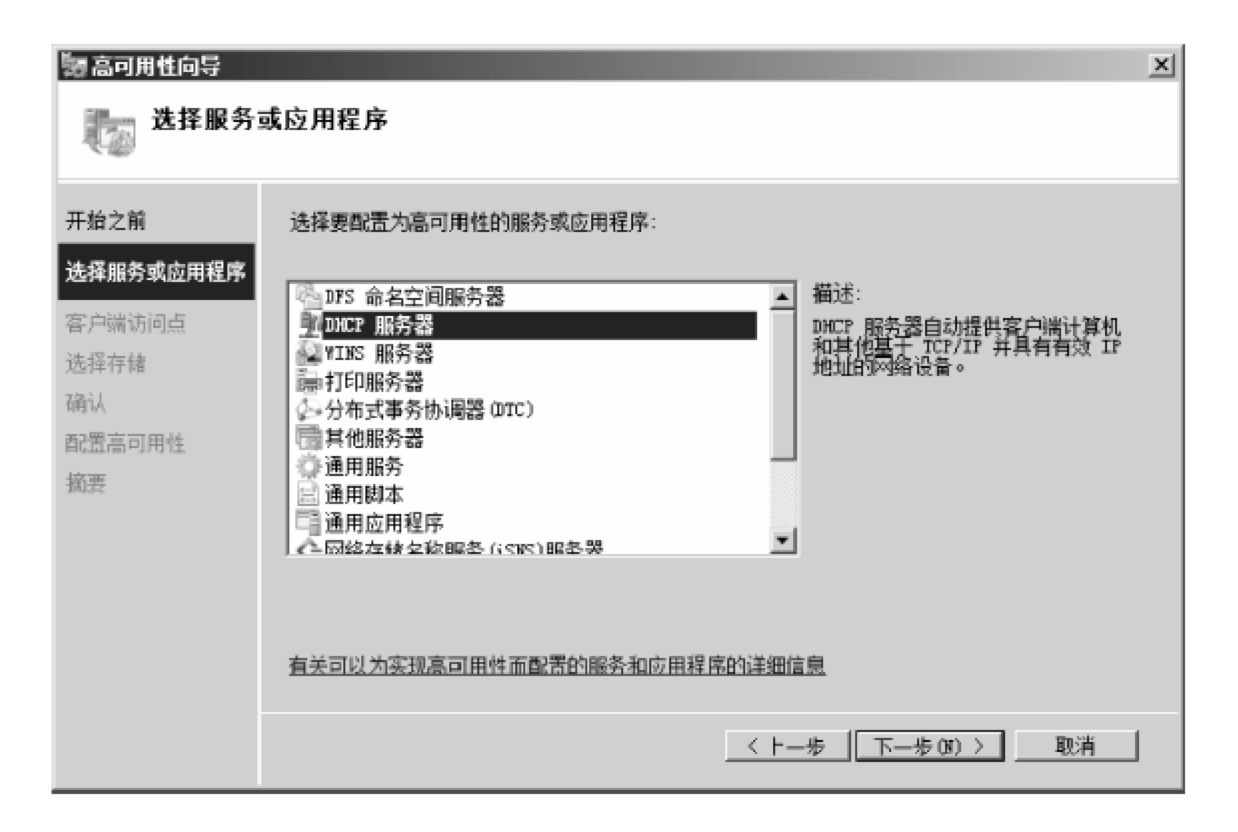


图 13-3 “选择服务或应用程序”对话框

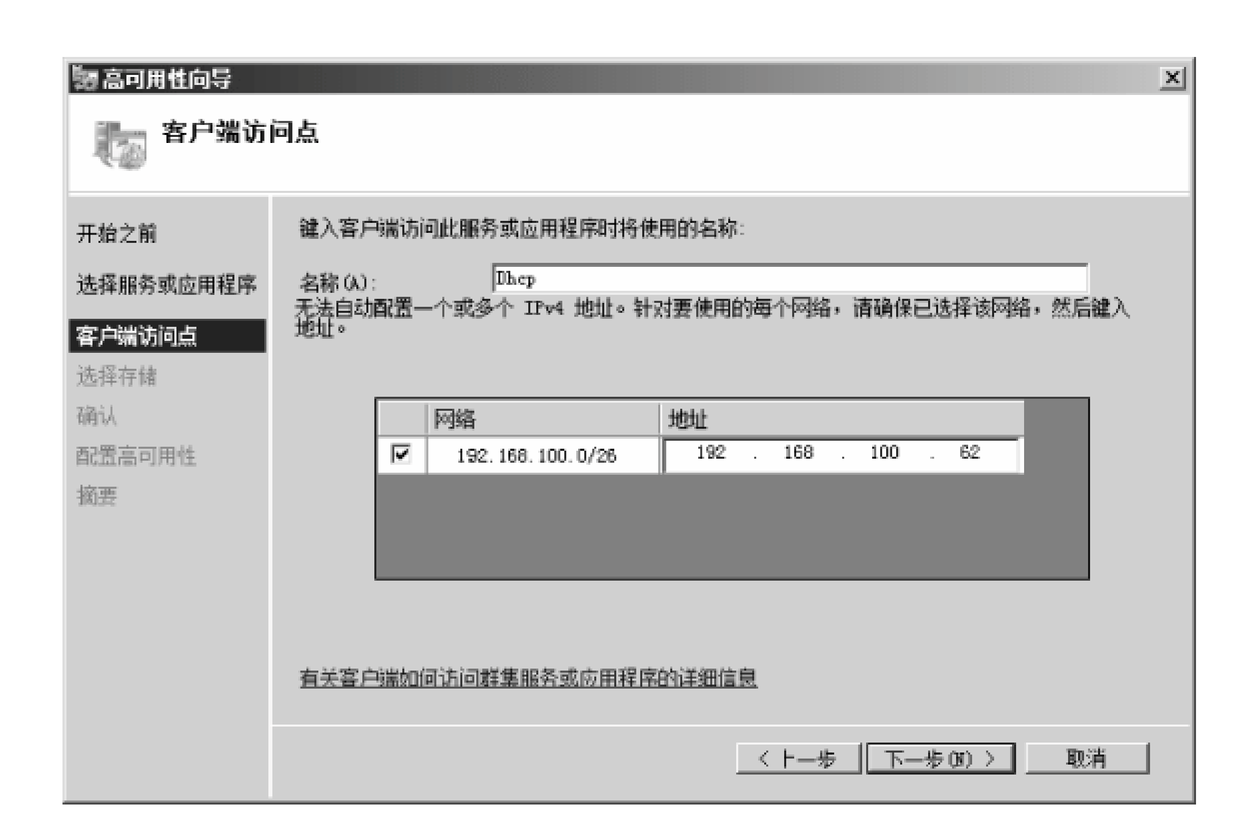


图 13-4 “客户端访问点”对话框

(4) 单击“下一步”按钮，显示如图 13-5 所示的“选择存储”对话框。选择希望分配给 DHCP 服务的存储卷，这里选择“群集磁盘 2”选项。

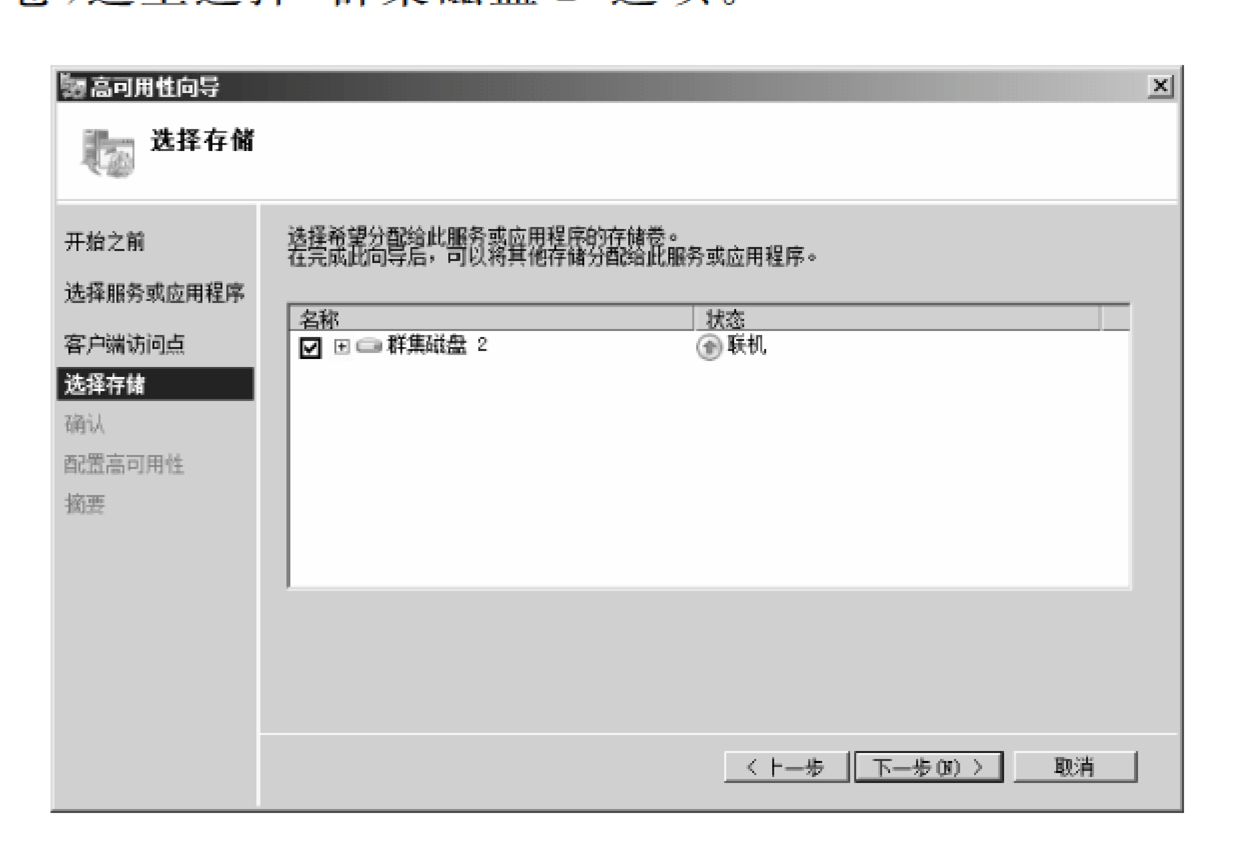


图 13-5 “选择存储”对话框

(5) 单击“下一步”按钮，显示如图 13-6 所示的“确认”对话框，提示已准备好为 DHCP 服务器配置高可用性。

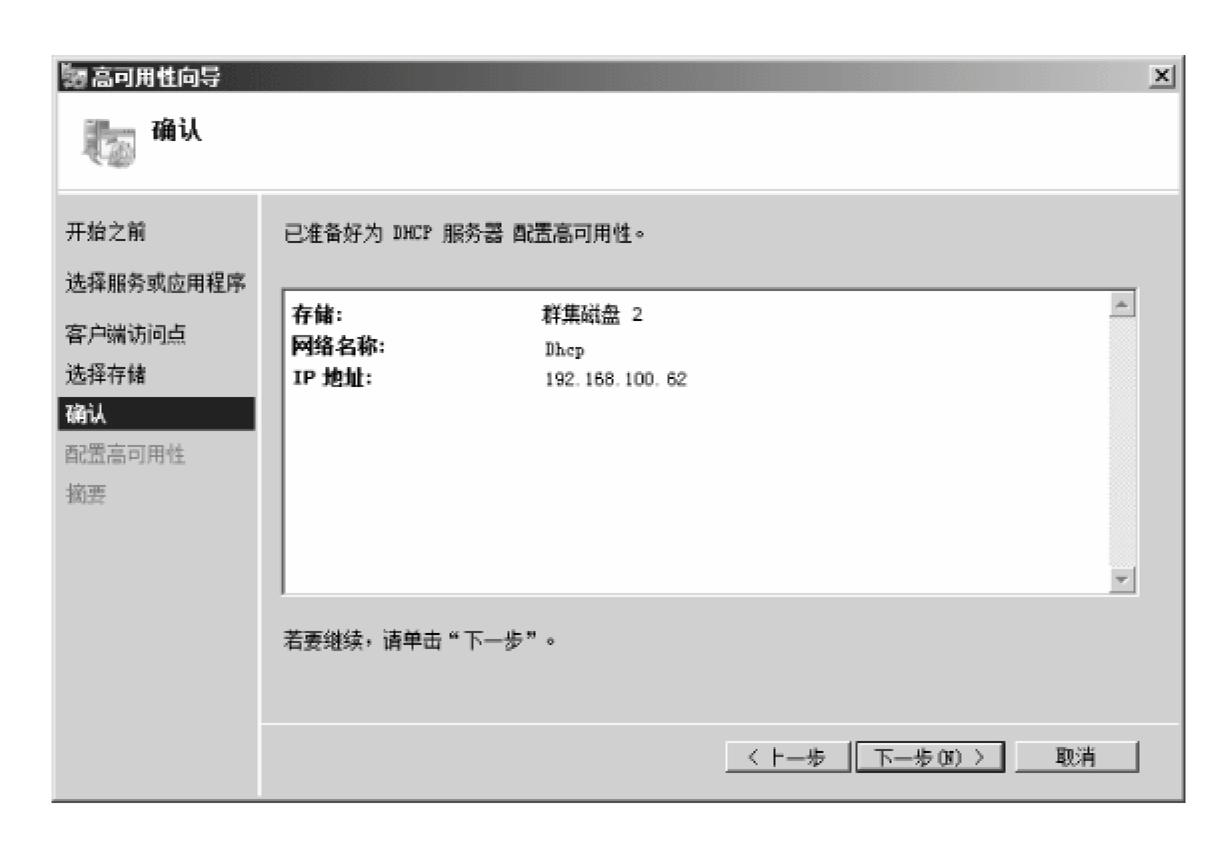


图 13-6　"确认"对话框

(6) 单击"下一步"按钮，开始配置 DHCP 服务器群集，配置完成后显示如图 13-7 所示的"摘要"对话框。如果想要查看详细的配置报告，可以单击"查看报告"按钮进行查看。



图 13-7　"摘要"对话框

(7) 单击"完成"按钮，完成 DHCP 服务器角色的配置。配置完成的 DHCP 服务器角色如图 13-8 所示。

4. 配置 DHCP 作用域

在 DHCP 服务器中，通过 IP 作用域为基本管理单位向客户端提供 IP 地址分配服务。管理员首先需要为每个物理子网创建作用域，然后使用该作用域定义 DHCP 客户端所使用的参数。当在故障转移群集中配置作用域时，并不在 DHCP 管理器窗口来完成，而在"故障转移群集管理器"窗口中来完成。

(1) 打开"故障转移群集管理"窗口，在左侧栏中依次展开"故障转移群集管理"→coolpen.coolpen.net→"服务和应用程序"→Dhcp 选项，在右侧"操作"栏中，单击"管理 DHCP"按钮，启动"故障转移群集管理"DHCP 服务器管理控制台，如图 13-9 所示。默认情况下，DHCP 服务器并没有得到授权，此时，DHCP 服务器还不能为网络提供服务。

(2) 右击 dhcp.coolpen.net，在快捷菜单中选择"授权"选项。依次展开 dhcp.coolpen.net→IPv4 选项，右击 IPv4 并在快捷菜单中选择"新建作用域"选项，显示如图 13-10 所示的



图 13-8 完成 DHCP 服务器的创建

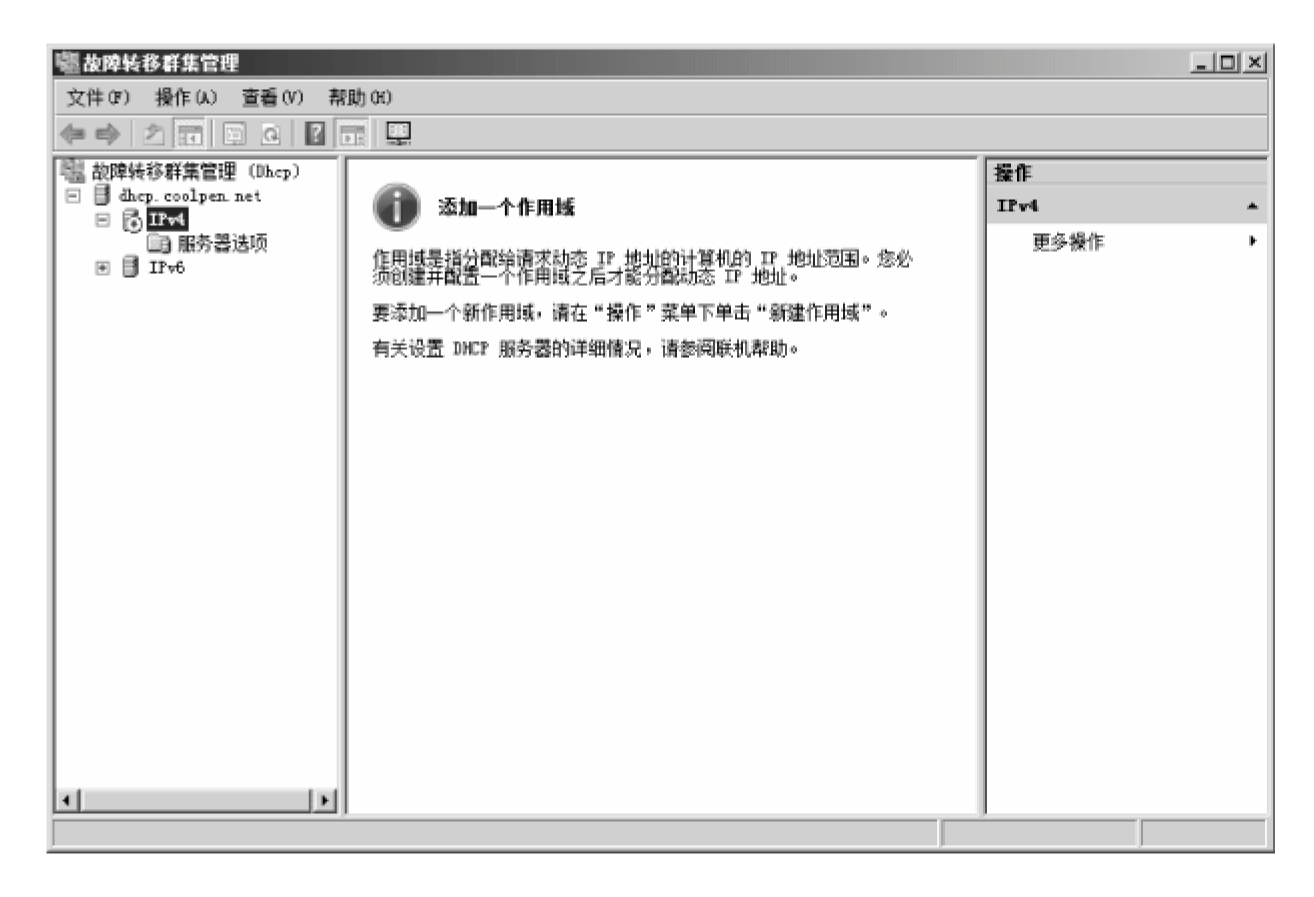


图 13-9 管理 DHCP

“欢迎使用新建作用域向导”对话框。

（3）单击“下一步”按钮，显示如图 13-11 所示的“作用域名称”对话框。分别在“名称”和“描述”文本框中，输入新建作用域的名称和描述信息。

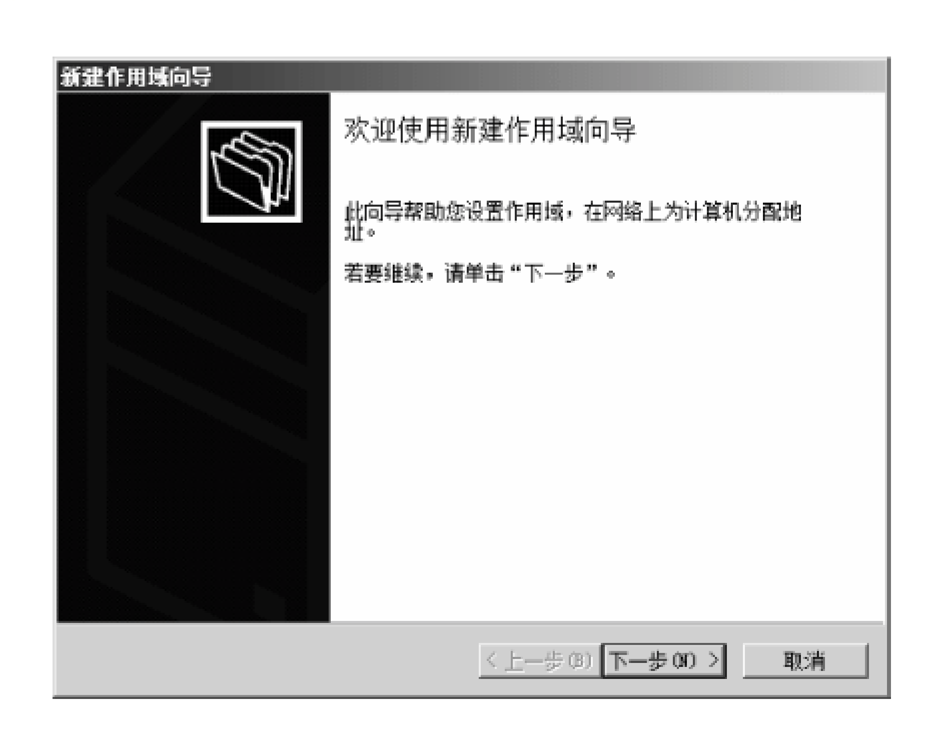


图 13-10 “欢迎使用新建作用域向导”对话框

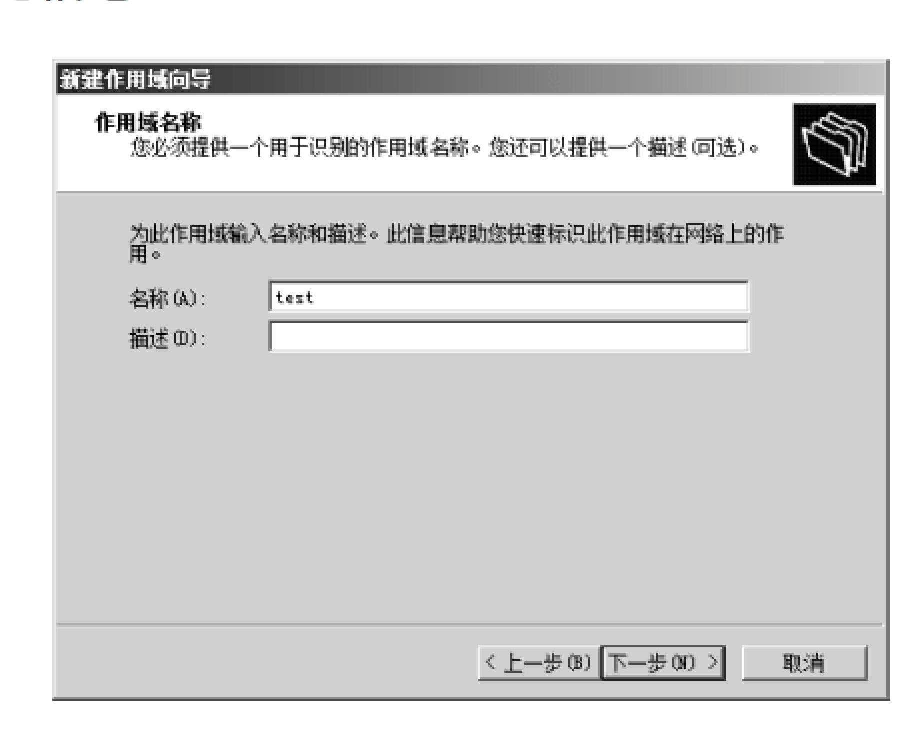


图 13-11 “作用域名称”对话框

（4）单击“下一步”按钮，显示如图13-12所示的“IP地址范围”对话框。分别在“起始IP地址”和“结束IP地址”文本框中，输入DHCP服务器提供的有效IP地址段。在“子网掩码”文本框中，输入该IP地址的子网掩码。

（5）单击“下一步”按钮，显示如图13-13所示的“添加排除”对话框。分别在“起始IP地址”和“结束IP地址”文本框中，输入欲排队的IP地址段。然后，单击“添加”按钮，将其添加到“排除的地址范围”列表中。

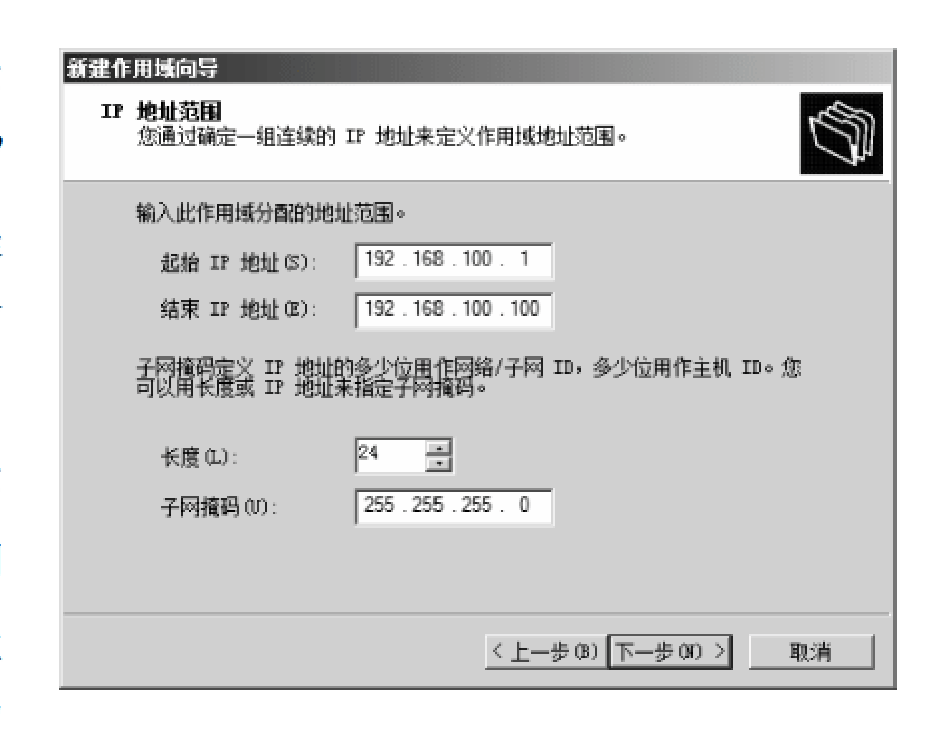


图13-12　“IP地址范围”对话框

（6）单击“下一步”按钮，显示如图13-14所示的“租用期限”对话框。根据实际需要，设置IP地址的租用期限，这里限制时间为5天。

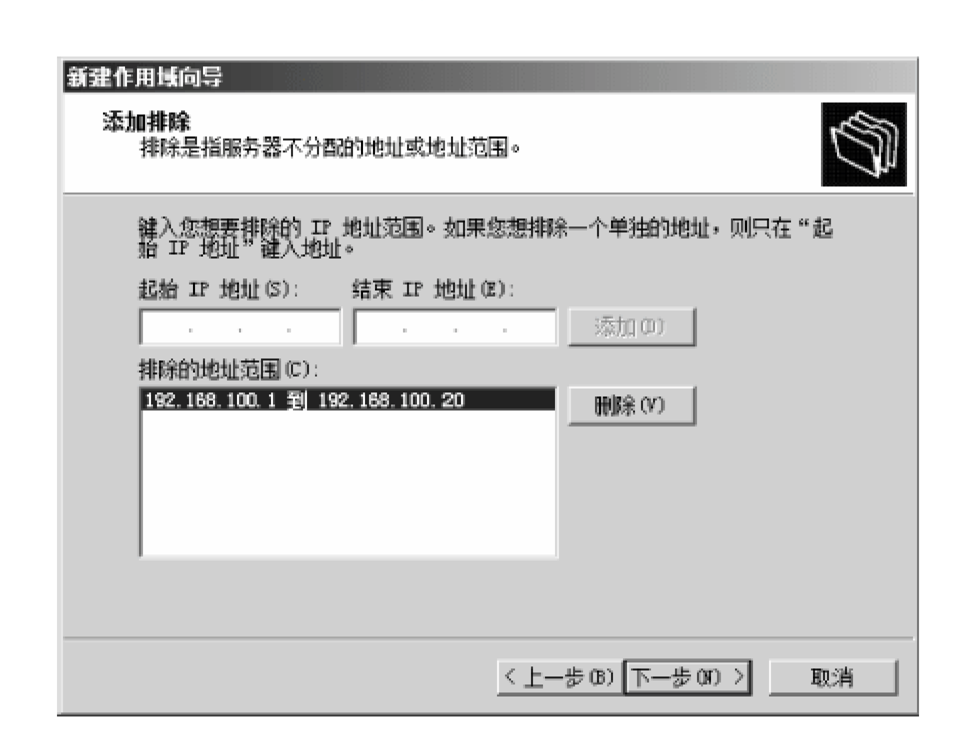


图13-13　“添加排除”对话框

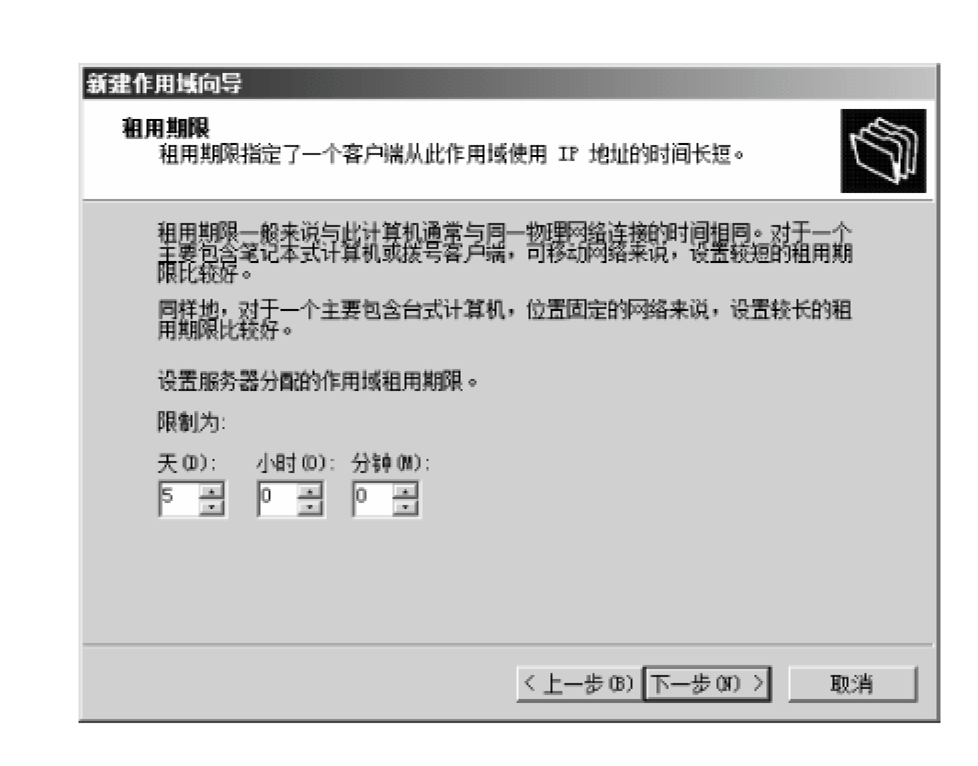


图13-14　“租用期限”对话框

（7）单击“下一步”按钮，显示如图13-15所示的“配置DHCP选项”对话框。如果想要继续配置网关参数，可以选中“是，我想现在配置这些选项”单选按钮。这里选中“否，我想稍后配置这些选项”单选按钮，在完成向导后再进行设置。

（8）单击“下一步”按钮，显示如图13-16所示的“正在完成新建作用域向导”对话框。提示已成功完成了新作用域的创建，在客户端接受地址前，还需要激活作用域。

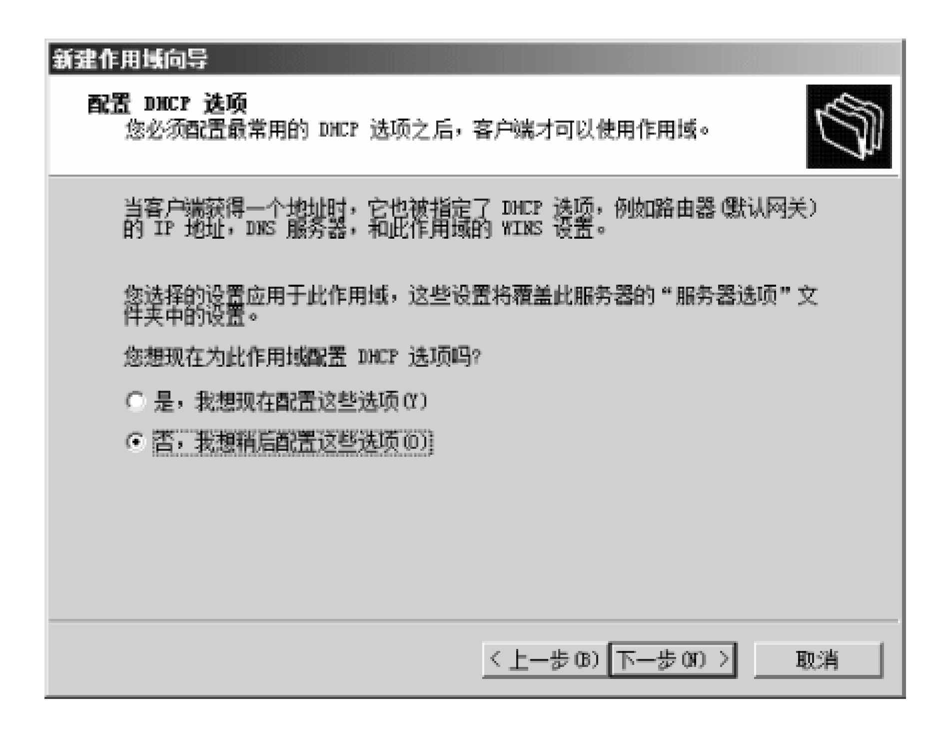


图13-15　“配置DHCP选项”对话框

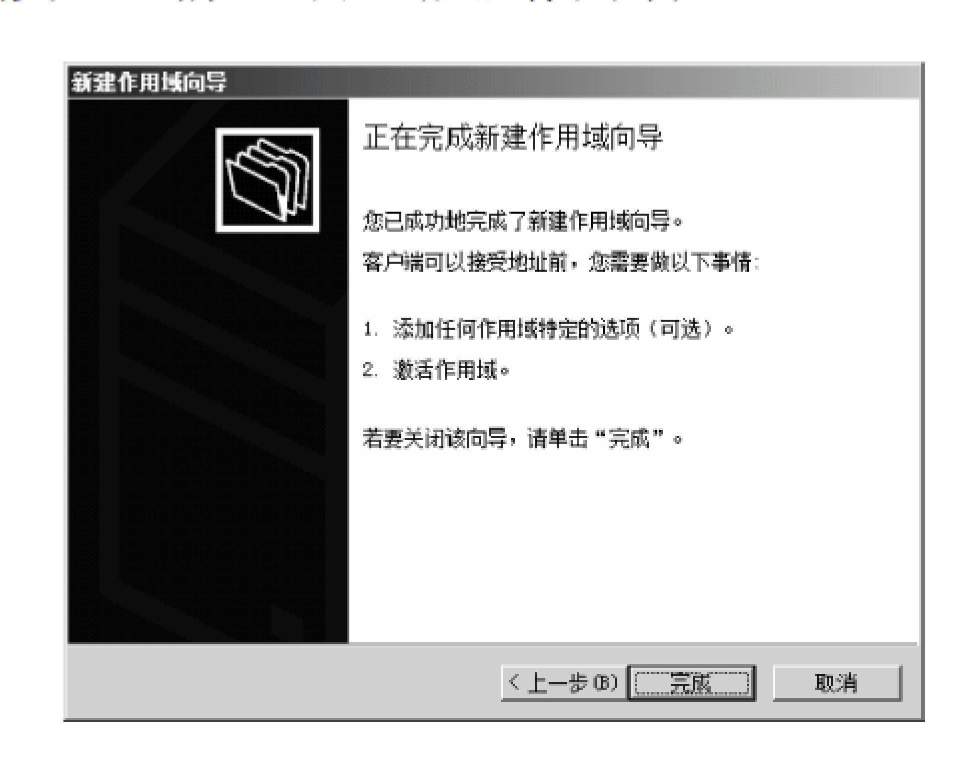


图13-16　“正在完成新建作用域向导”对话框

(9) 单击“完成”按钮,完成新作用域的创建,如图 13-17 所示。

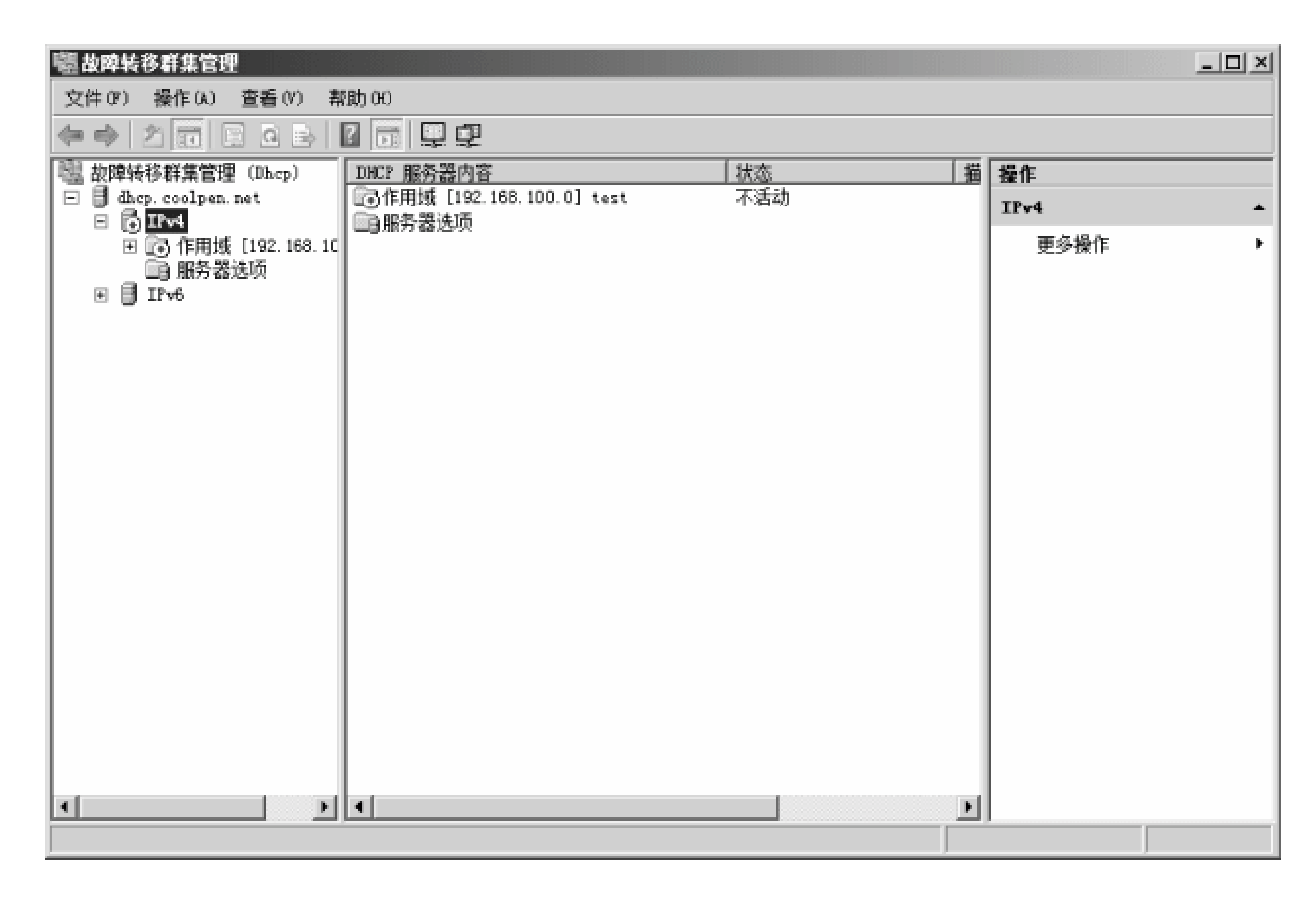


图 13-17 完成新作用域的创建

(10) 右击新建的作用域,在快捷菜单中选择“激活”选项。激活新建的作用域,如图 13-18 所示。此时,该 DHCP 服务器即可为客户端计算机提供 IP 地址的分配工作。

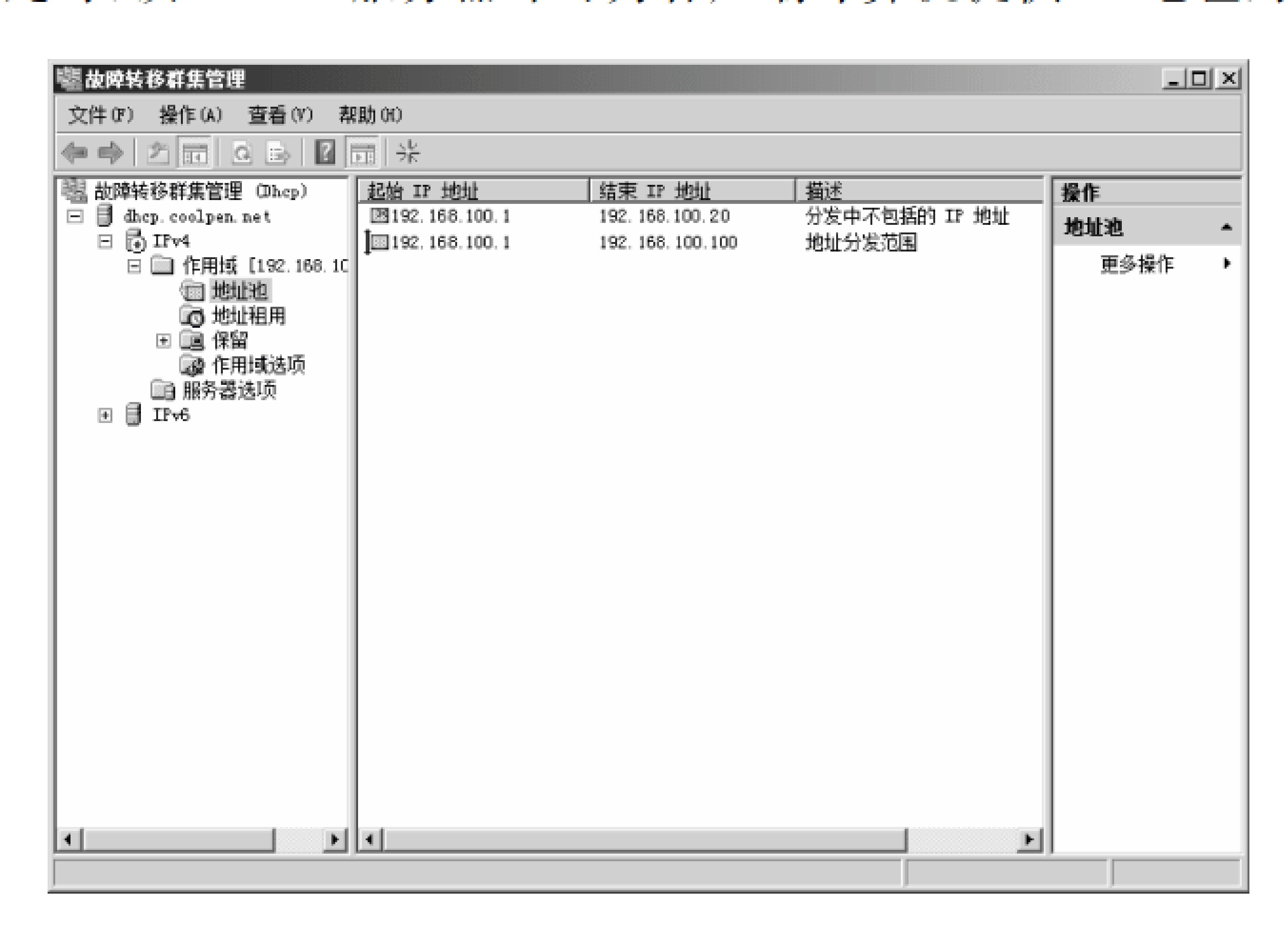


图 13-18 激活作用域

5. DHCP 群集测试

群集部署成功后,为了确认服务器可以实现故障转移,可以模拟当某台群集成员服务器发生故障时,其他成员服务器可以继续这台服务器的工作。具体操作步骤如下。

(1) 在“故障转移群集管理”窗口中,依次展开“故障转移群集管理”→coolpen. coolpen. net→“服务和应用程序”→Dhcp 选项,如图 13-19 所示。从图中可知,此时的所有者为 files2。

(2) 将 files2 关机或断开网络,在另一台成员服务器上,启动“故障转移群集管理”,再次查看当前群集的所有者,可发现此时的所有者为 files1,如图 13-20 所示,即表示群集故障自动转移成功。



图 13-19　查看当前所有者



图 13-20　成功转移故障

13.2.2　配置负载均衡

网络负载均衡(NLB)可以让客户端用一个逻辑 Internet 名称和虚拟 IP 地址(又称群集 IP 地址)访问群集,同时保留每台计算机各自的名称。管理员可以通过 Windows Server 2008 中的网络负载均衡功能,实现 Web 服务器、FTP 服务器、ISA 服务器等关键应用服务的负载均衡,从而提升网络的可靠性。

1. 准备工作

在 Windows Server 2008 系统中配置 NLB 之前,必须完成必要的准备工作。

(1) 设置网卡属性。在每个节点采用相同的方式安装和配置网卡。通常情况下,每个节点的每块网卡的所有属性都应当设置为相同值,包括网卡传输速度、模式、流控制和媒体类型等。

（2）选择网络协议。所有网卡都必须取消对 NetBIOS over TCP/IP 选项（位于 WINS 选项卡）的选择，并且使 TCP/IP 协议成为连接专用网络网卡的唯一网络协议。

（3）设置 IP 地址信息。公用网卡用于响应客户端用户对网络服务器的访问，专用网卡用于服务器群集中节点间的通信。建议不要使用 DHCP 为任何网卡分配 IP 地址，而应当为所有网卡指定静态 IP 地址信息。

（4）安装 NLB。NLB 功能默认并未安装和启用，在 Windows Server 2008 系统中，管理员可以通过添加"功能"的方式安装 NLB。需要注意的是，在安装 NLB 前，必须配置要安装 NLB 的适配器上只有 TCP/IP，不能向该适配器中添加任何其他协议。

（5）用户权限配置。使用 NLB 管理器时，必须是正在配置的主机上的 Administrators 组的成员，或者被委派了适当权限的用户。如果通过不属于群集的计算机运行 NLB 管理器来配置群集或主机，则不必是该计算机 Administrators 组的成员。

2. 新建网络负载均衡群集

（1）依次选择"开始"→"管理工具"→"网络负载均衡管理器"选项，即可启动"网络负载平衡管理器"。右击"网络负载平衡群集"，在快捷菜单中选择"新建群集"选项，显示如图 13-21 所示的"新群集：连接"对话框。在"主机"文本框中，输入欲添加的主机的 IP 地址。单击"连接"按钮，即可开始连接到群集计算机。在"可用于配置新群集的接口"列表中，显示该主机可用的网络连接，并选中所要使用的网络连接接口。



图 13-21 "新群集：连接"对话框

（2）单击"下一步"按钮，显示如图 13-22 所示的"新群集：主机参数"对话框。在"优先级（单一主机标识符）"下拉列表框中，选择所要使用的某个值。该参数为每个主机指定一个唯一 ID。在"默认状态"下拉列表框中，可以选择设置完成后，该群集的状态默认为"已启动"。如果选中"在计算机重新启动后保持挂起状态"复选框，可以在群集计算机重新启动后，保持挂起状态，直到管理员手动启动。

（3）单击"下一步"按钮，显示如图 13-23 所示的"新群集：群集 IP 地址"对话框。在该对话框中，根据需要设置群集的每个成员所共享的群集 IP 地址，即负载平衡时所使用的 IP 地址。



图 13-22　“新群集：主机参数”对话框



图 13-23　“新群集：群集 IP 地址”对话框

（4）单击“添加”按钮，显示如图 13-24 所示的“添加 IP 地址”对话框。因为这里只使用 IPv4 地址，所以只能选中“添加 IPv4 地址”单选按钮。在“IPv4 地址”和“子网掩码”文本框中，分别输入想要设置的 IP 地址和子网掩码。

（5）单击“确定”按钮，返回“新群集：群集 IP 地址”对话框，单击“下一步”按钮，显示如图 13-25 所示的“新群集：群集参数”对话框。根据需要，选择“IP 地址和子网掩码”中的值，在“完整 Internet 名称”文本框中，输入用户将用于访问该 NLB 群集的 Internet 全名。在“群集操作模式”中，选择所要使用的群集操作模式，这里保持默认设置，即使用“单播”模式。在单播模式中，会将群集的 MAC 地址指定给计算机的网络适配器，不使用网络适配器的内置 MAC 地址。



图 13-24　“添加 IP 地址”对话框



图 13-25　“新群集：群集参数”对话框

（6）单击“下一步”按钮，显示如图 13-26 所示的“新群集：端口规则”对话框。在该对话框中，可以根据需要修改端口规则，单击“编辑”按钮进行修改即可，这里保持默认设置。

（7）单击“完成”按钮，完成设置。稍等片刻，即可成功创建群集，并将该主机添加到群集中。

3. 向群集中添加主机

通常情况下，群集的计算机可能会有多台，为了使所提供的服务更加稳定，可以向群集中添加更多的主机。具体操作步骤如下。

（1）在“网络负载平衡管理器”窗口中，右击群集名称，在快捷菜单中选择“添加主机到群集”选项，显示如图 13-27 所示的“将主机添加到群集：连接”对话框。在“主机”文本框中，输入想要添加的主机 IP 地址，单击“连接”按钮，即可连接到该主机。



图 13-26 “新群集：端口规则”对话框



图 13-27 “将主机添加到群集：连接”对话框

（2）单击“下一步”按钮，显示如图 13-28 所示的“将主机添加到群集：主机参数”对话框。具体设置方法同“新建网络负载平衡群集”，这里不再赘述。

（3）单击“下一步”按钮，显示如图 13-29 所示的“将主机添加到群集：端口规则”对话框。根据需要进行设置即可，这里保持默认设置。



图 13-28 “将主机添加到群集：主机参数”对话框

图 13-29 “将主机添加到群集：端口规则”对话框

（4）单击“完成”按钮，完成主机的添加。

13.2.3 知识链接：故障转移群集和网络负载均衡

1. 故障转移群集的优缺点

故障转移群集具备以下优点。

（1）适应计划内的停机时间。故障转移群集可以允许系统有停机时间，而不会影响可用性，满足日常维护和升级需要。

（2）减少计划外停机时间。故障转移群集通过消除系统和应用程序级别上的故障单点，减少服务器和软件故障有关的应用程序停机时间。

故障转移群集具备以下缺点。

(1) 增加响应时间。对于故障转移群集设计来说,由于备用服务器上的负载增长,或需要更新多台服务器的状态信息,因此会增加响应时间。

(2) 增加设备成本。故障转移群集所要求的额外硬件使购买服务器以及相应软件的成本加倍。

2. 网络负载均衡的功能

Windows Server 2008 系统的网络负载均衡提供如下功能。

(1) 可伸缩性

可伸缩性是度量计算机、服务或应用程序如何更好地改进以满足持续增长的性能需求的标准。对于 NLB 群集而言,可伸缩性是指当群集的全部负载超过其能力时逐步将一个或多个系统添加到现有群集中的功能。NLB 的可伸缩性功能包括如下内容。

① 平衡 NLB 群集上对各个 TCP/IP 服务的负载请求。

② 在一个群集中最多支持 32 台计算机。

③ 平衡群集中多个主机之间的多个服务器负载请求(来自同一个客户端或者来自几个客户端)。

④ 支持在负载增加时,能够在不关闭群集的情况下向 NLB 群集中添加主机。

⑤ 支持在负载降低时,能够从群集中删除主机。

⑥ 通过全部实现管道化提高性能并降低开销。管道允许向 NLB 群集发送请求,而无须等待响应上一个发送的请求。

(2) 高可用性

通过最大限度地减少停机时间,高可用系统能够可靠地提供可接受级别的服务。NLB 包括一些内置功能,可以通过自动执行以下操作来提供高可用性。

① 检测发生故障或脱机的群集主机并对其进行恢复。

② 在添加或删除主机时平衡网络负载。

③ 在 10s 之内恢复并重新分发负载。

(3) 可管理性

NLB 提供以下可管理性功能。

① 使用 NLB 管理器,可以从单个计算机管理和配置多个 NLB 群集和群集主机。

② 使用端口管理规则,可以为单个 IP 端口或一组端口指定负载平衡行为。

③ 可以为每个网站定义不同的端口规则。如果对多个应用程序或网站使用相同的一组负载平衡服务器,则端口规则基于目标虚拟 IP 地址(使用虚拟群集)。

④ 使用可选的单主机规则,可以将所有客户端请求引导至单个主机。NLB 将客户端请求路由到运行特定应用程序的特定主机。

⑤ 可以阻止对某些 IP 端口进行不需要的网络访问。

⑥ 可以在群集主机上启用 Internet 组管理协议(IGMP)支持,以控制交换机广播(在多播模式中操作时)。

⑦ 使用 shell 命令或脚本,可以从运行 Windows 的任何联网计算机上远程启动、停止和控制 NLB 操作。

⑧ 可以查看 Windows 事件日志以检查 NLB 事件。NLB 在事件日志中记录所有操作

和群集更改。

(4) 易用性

NLB 提供了许多便于使用的功能。

① 可以作为标准的 Windows 网络驱动程序组件安装 NLB。

② NLB 不需要更改任何硬件即可启用和运行。

③ 使用 NLB 管理器可以新建 NLB 群集。

④ 使用 NLB 管理器,可以从一台远程或本地计算机上配置和管理多个群集以及群集的所有主机。

⑤ NLB 允许客户端使用单个逻辑 Internet 名称和虚拟 IP 地址(称为群集 IP 地址,保留每台计算机的各个名称)访问群集。NLB 允许多宿主服务器具有多个虚拟 IP 地址。需要注意的是,如果是虚拟群集,则不需要服务器是多宿主服务器即可具有多个虚拟 IP 地址。

⑥ 可以将 NLB 绑定到多个网络适配器,这样便可以在每个主机上配置多个独立的群集。支持多个网络适配器与虚拟群集不同,因为虚拟群集允许在单个网络适配器上配置多个群集。

⑦ 不需要修改服务器应用程序即可在 NLB 群集中运行。

⑧ 如果群集主机出现故障并且后来又恢复联机,则可以将 NLB 配置为自动将该主机添加到群集。然后,添加的主机将能够开始处理来自客户端的新的服务器请求。

⑨ 可以在不打扰其他主机上群集操作的情况下使计算机脱机进行预防性的维护。

13.3 网络链路冗余

网络链路冗余是增加传输带宽、提高网络可靠性的常用物理方法。任何厂商都不能保证其产品不发生故障,而发生故障时能否迅速切换到一个好设备上,是令人关心的问题。与服务器的网卡冗余类似,网络传输达到或超过带宽限制时,可以通过网络链路负载均衡功能,将负载平均分配到所有链路上,从而提高了传输速率。如果主链路出现故障,则备用链路仍可继续工作,以保证网络传输的正常进行。

13.3.1 配置交换机链路汇聚

借助于 PAgP 或 LACP 协议,可以很容易地在支持 EtherChannel 功能的端口之间,自动建立 Fast EtherChannel 和 Gigabit EtherChannel 连接。图 13-30 所示为在 Cisco Catalyst 2960 和 Catalyst 3750 之间创建的拥有 2 条链路的 Gigabit EtherChannel,实现链路汇聚。

提示:只有在固定端口(如双绞线端口或光纤端口)之间才可以创建 EtherChannel,而由 GBIC 或 SFP 插槽所创建的链路是不能用于创建 EtherChannel 的。

链路汇聚技术在网络中的实际应用是非常广泛的。可以将 10/100Mbps 端口或交换机,聚合为千兆连接,轻松获得快速的网络传输。而对于千兆端口或交换机而言,断口汇聚则可以成倍增加网络干路的带宽,消除交换机级联产生的网络瓶颈。不仅如此,断口汇聚技术还可以应用于服务器到骨干交换机的连接,如图 13-31 所示,不仅突破了服务器到交换机千兆传输速率的限制,还可以实现多网卡的负载均衡,充分保障了网络访问的可靠性。

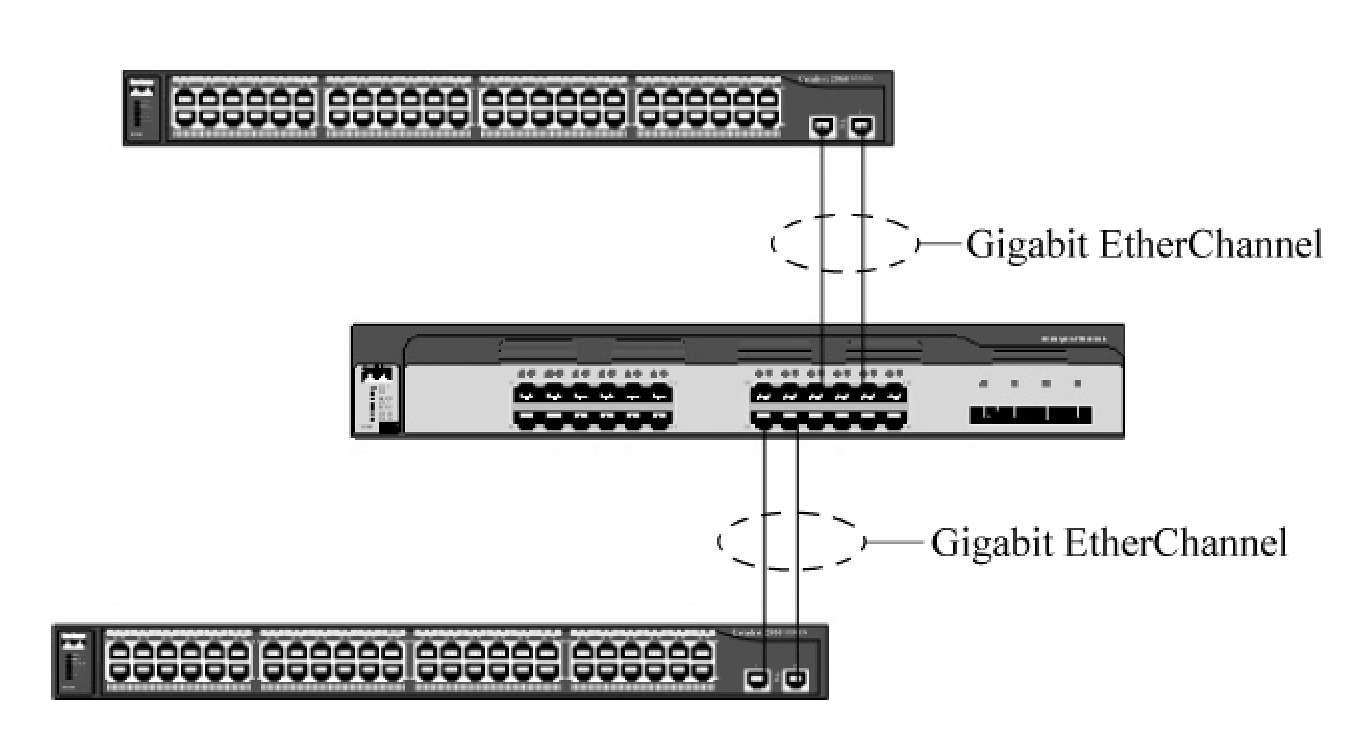


图 13-30　Gigabit EtherChannel

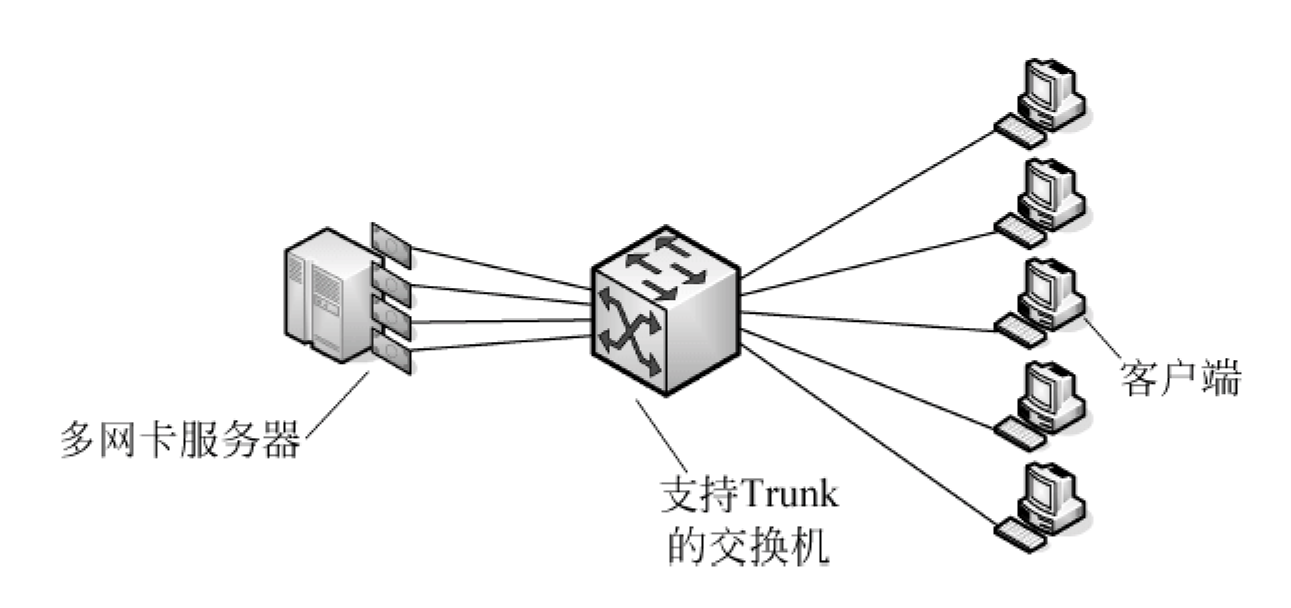


图 13-31　Trunk 技术解决交换机和服务器之间的传输瓶颈

1．创建 EtherChannel

（1）进入配置模式。

```
Switch# configure terminal
```

（2）选择欲配置为 EtherChannel 的物理接口。PAgP EtherChannel 组可以容纳 8 个(4 对)同一类型和速度的端口。LACP EtherChannel 组最多可以容纳 16 个(8 对)相同类型的端口，其中 8 个(4 对)活动端口，以及最多 8 个(4 对)备用端口。

```
Switch(config)# interface interface-id
```

（3）将所有端口指定为同一 VLAN 内的静态访问端口，或者配置为 Trunk。如果配置为静态端口，只能指定至一个 VLAN，VLAN 的取值范围为 1～4094。

```
Switch(config-if)# switchport mode{access|trunk}switchport access vlan vlan-id
```

（4）将接口指定至 EtherChannel 组，并指定 PAgP 或 LACP 模式。EtherChannel 端口组的取值范围为 1～48。channel-group 命令的参数及用法如表 13-1 所示。

```
Switch(config-if)# channel-group port_channel_number mode{{auto[non-silent]|desirable[non-silent]|on}|{active|passive}}
```

采用 PAgP 协议时，以下两种模式可以构建 EtherChannel。

① 一个接口为 desirable 模式；另一个接口为 desirable 或 auto 模式。

② 一个接口为 auto 模式；另一个接口为 desirable 模式。

表 13-1 channel-group 命令的参数及用法

参　　数	描　　述
auto	当侦测到 PAgP 设备时，将只启用 PAgP。将端口置于被动协商状态，可以对接收到的 PAgP 做出响应，但是，不能主动发送 PAgP 包进行协商
desirable	无条件启用 PAgP。将接口置于主动协商状态，通过发送 PAgP 包，主动与其他接口进行协商
on	将接口强行指定至 Channel。只有两个 on 模式接口组连接时，EtherChannel 才可用
non-silent	如果交换机连接到有 PAgP 能力的伙伴，可以将接口配置为 non silent(非沉默)运行。如果没有为 auto 或 desirable 模式指定 non-silent 关键字，默认为 silent。沉默设置被用于连接到文件服务器或包分析仪。该设置允许 PAgP，将接口添加至 Channel 组，并使用接口进行传输
active	当侦测到 LACP 设备时，将只启用 LACP。激活接口的主动协商状态，通过发送 LACP 包，与其他接口进行主动协商
passive	当侦测到 LACP 设备时，将只启用 LACP。将端口置于被动协商状态，可以对接收到的 LACP 作出响应，但是，不能主动发送 LACP 包进行协商

采用 LACP 协议时，以下两种模式可以构建 EtherChannel。

① 一个接口为 active 模式；另一个接口为 active 或 passive 模式。

② 一个接口为 active 模式；另一个接口为 passive 模式。

(5) 退出配置模式。

```
Switch(config-if)# end
```

(6) 校验配置。

```
Switch# show running-config
```

(7) 保存配置。

```
Switch# copy running-config startup-config
```

提示：GBIC 和 SFP 接口不能被配置为 EtherChannel。

2. 配置 EtherChannel 负载均衡

EtherChannel 还具有负载均衡和线路备份的功能，建议创建 EtherChannel 链路汇聚后，立即配置，以增强网络的稳定性和安全性。主要操作步骤如下。

(1) 进入配置模式。

```
Switch# configure terminal
```

(2) 配置 EtherChannel 负载均衡。

```
Switch(config)# port-channel load-balance{dst-mac|src-mac}
```

提示：dst-mac，基于进入包的目的主机的 MAC 地址进行负载分配。src-mac，基于进入包的源 MAC 地址进行负载分配。

(3) 退出配置模式。

```
Switch(config-if)# end
```

(4) 校验配置。

```
Switch# show etherchannel load-balance
```

（5）保存配置。

```
Switch# copy running-config startup-config
```

3. 从 EtherChannel 中移除接口

从 EtherChannel 中移除接口的主要操作步骤如下。

（1）进入配置模式。

```
Switch# configure terminal
```

（2）指定欲配置的物理接口。

```
Switch(config)# interface interface-id
```

（3）从 EtherChannel 中移除接口。

```
Switch(config-if)# no channel-group
```

（4）退出配置模式。

```
Switch(config-if)# end
```

（5）校验配置。

```
Switch# show running-config
```

（6）保存配置。

```
Switch# copy running-config startup-config
```

4. 移除 EtherChannel

移除 EtherChannel 后所有端口将恢复原始状态，主要操作步骤如下。

（1）进入配置模式。

```
Switch# configure terminal
```

（2）移除 Channel 接口。

```
Switch(config)# no interface port-channel port_channel_number
```

（3）退出配置模式。

```
Switch(config-if)# end
```

（4）校验配置。

```
Switch# show etherchannel summary
```

（5）保存配置。

```
Switch# copy running-config startup-config
```

13.3.2　配置交换机链路冗余

配置 Spanning Tree 与 EtherChannel 有所不同，它只能保证在两台交换机之间拥有一

条活动链路，备用链路只有在主链路出现故障时才会启用。

1. 禁用 Spanning Tree

交换机的 Spanning Tree 功能默认是开启的，如果确认在 VLAN 内没有拓扑环，可以将其禁用，以减少端口接入时等待的时间。主要操作步骤如下。

(1) 进入配置模式。

```
Switch# configure terminal
```

(2) 在指定 VLAN 内禁用 Spanning Tree。

```
Switch(config)# no spanning-tree vlan vlan-id
```

(3) 返回至特权配置模式。

```
Switch(config-if)# end
```

(4) 查看并校验配置。

```
Switch# show spanning-tree vlan vlan-id
```

(5) 保存配置。

```
Switch# copy running-config startup-config
```

若欲重新启用 STP，可以使用 spanning-tree vlan vlan-id 全局配置命令。

2. 将交换机配置为根交换机

当 VLAN 中存在有拓扑环时，应当通过根交换机、端口优先级和路径费用等设置，确定网络拓扑结构，从而使 Spanning Tree 的生成时间最短。

(1) 进入配置模式。

```
Switch# configure terminal
```

(2) 将交换机配置为指定 VLAN 的根交换机。diameter net-diamete 用于指定两个终端间交换机的数量，取值范围为 2～7。使用 spanning-tree vlan vlan_id root secondary diameter net-diamete 命令，可以将交换机配置为次根交换机。

```
Switch(config)# spanning-tree vlan vlan_id root primary diameter net-diamete
```

(3) 返回至特权配置模式。

```
Switch(config-if)# end
```

(4) 查看并校验配置。

```
Switch# show spanning-tree detail
```

(5) 保存配置。

```
Switch# copy running-config startup-config
```

若欲将交换机恢复为默认配置，可以在全局配置模式下使用 no spanning-tree vlan vlan-id root 命令。

3. 配置端口优先值

如果 VLAN 内有拓扑环，Spanning Tree 将使用端口优先值确定将哪个接口置于转发状态，因此，可以为欲首先选择的端口赋予较高优先级值(较小的数值)。如果所有端口都有相同的优先级值，那么，具有最小端口号的端口将被设置为转发状态，其他接口则处于阻塞状态。

(1) 进入配置模式。

```
Switch# configure terminal
```

(2) 选择欲配置的接口，既可以是物理接口，也可以是 EtherChannel 逻辑端口(port-channel port-channel-number)。

```
Switch(config)# interface interface-id
```

(3) 为接口配置优先级值，取值范围为 0～255，默认值为 128。数值越低，优先级越高。

```
Switch(config-if)# spanning-tree port-priority priority
```

(4) 为接口配置 VLAN 端口优先级。取值范围为 0～255，默认值为 128。数值越低，优先级越高。

```
Switch(config-if)# spanning-tree vlan vlan-id port-priority priority
```

(5) 返回特权配置模式。

```
Switch(config)# end
```

(6) 校验配置。

```
Switch# show spanning-tree interface interface-id|{port-channel port_channel_number}
Switch# show spanning-tree vlan vlan_id
```

(7) 保存配置。

```
Switch# copy running-config startup-config
```

使用 no spanning-tree [vlan vlan-id] port-priority 接口配置命令，可以将端口优先级恢复为默认值。

4. 配置路径费用

Spanning Tree 路径费用的默认值取决于接口的类型与速率。当 VLAN 中有拓扑环时，Spanning Tree 使用路径费用选择将哪个接口置于转发状态。具有最低端口费用的端口将被选择用于向所有的 VLAN 转发帧。因此，可以为欲选择的接口赋予较低的费用值，以确定网络拓扑。通常情况下，应当为快速链路(如 1000Mbps 端口)赋予一个最小值，而为一个慢速链路(如 100Mbps 端口)赋予一个最大值。如果所有接口的成本值都有相同，那么，具有最小端口号的端口将被设置为转发状态，其他接口则处于阻塞状态。

(1) 进入配置模式。

```
Switch# configure terminal
```

（2）选择欲配置的接口，既可以是物理接口，也可以是 EtherChannel 逻辑端口（port-channel port-channel-number）。

```
Switch(config)# interface interface-id
```

（3）配置接口的费用，取值范围为 1～200000000。较低的路径费用表明有较高的传输速率。

```
Switch(config-if)# spanning-tree cost cost
```

（4）配置 VLAN 的费用，取值范围为 1～200000000。较低的路径费用表明有较高的传输速率。

```
Switch(config-if)# spanning-tree vlan vlan_id cost cost
```

（5）返回特权配置模式。

```
Switch(config)# end
```

（6）校验配置。

```
Switch# show spanning-tree interface{interface-id}|{port-channel port_channel_number}
Switch# show spanning-tree vlan vlan_ID
```

（7）保存配置。

```
Switch# copy running-config startup-config
```

使用 no spanning-tree [vlan vlan-id] cost 接口配置命令，可以将接口费用恢复为默认值。

13.3.3 配置三层交换机路由冗余

1. 启用 HSRP

在特权 EXEC 模式下开始，执行如下操作，可以在一个 3 层接口上创建或启用 HSRP。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）进入接口配置模式，并且进入欲启用 HSRP 的 3 层接口。

```
Switch(config)# interface interface-id
```

（3）创建 SHRP 组，利用组号或者虚拟 IP 地址。

```
Switch(config)# standby[group-number]ip[ip-address[secondary]]
```

（4）返回特权 EXEC 模式。

```
Switch(config)# end
```

（5）校验配置。

```
Switch# show standby[interface-id[group]]
```

（6）保存配置。

```
Switch(config)# copy running-config startup-config
```

使用 no standby [group-number] ip [ip-address]接口配置指令来禁用 HSRP。

2. 配置 HSRP 优先权

在特权 EXEC 模式下开始，借助以下操作，可以在接口上配置 HSRP 优先权。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）进入接口配置模式，并进入欲设置优先权的 HSRP 接口。

```
Switch(config)# interface interface-id
```

（3）设置被用于选择活动路由的优先值。范围是 1～255，默认的优先值是 100。数值越高，优先权越高。

```
Switch(config)# standby[group-number]priority priority[preempt [delay delay]]
```

（4）配置路由 to preempt，即当路由器比活动的路由有较高的优先权时，它便作为一个活动路由。

```
Switch(config)# standby[group-number][priority priority]preempt[delay delay]
```

（5）配置一个接口来追踪其他的接口，以便其他的某个接口失效时，设备的热备份优先权被降低。

```
Switch(config)# standby[group-number]track type number[interface-priority]
```

（6）返回特权 EXEC 模式。

```
Switch(config)# end
```

（7）校验配置。

```
Switch# show running-config
```

（8）保存配置。

```
Switch(config)# copy running-config startup-config
```

使用 no standby [group-number] priority priority [preempt [delay delay]] 和 no standby [group-number] [priority priority] preempt [delay delay]接口配置指令，重新存储默认优先权，preempt 和延迟值。

使用 no standby [group-number] track type number [interface-priority]接口配置指令移除追踪。

3. 配置 MHSRP

启用 MHSRP 负载平衡，配置两个路由作为活动路由，把虚拟路由器作为备份路由器。配置 MHSRP 时，需要在每个 HSRP 接口上输入 standby preempt 接口配置指令，以便如果其他路由器失效后返回。

路由器 A 被配置为 1 组的活动路由器，路由器 B 被配置为 2 组的活动路由器。路由器 A 的 HSRP 接口有一个 IP 地址 10.0.0.1，1 组的备份优先权是 110。路由 B 的 HSRP 接口的 IP 地址是 10.0.0.2，2 组的备份优先权是 110。

1 组使用虚拟 IP 地址 10.0.0.3，2 组使用虚拟 IP 地址 10.0.0.4。

配置路由 A：

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

配置路由 B：

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

4. 配置 HSRP 认证和时钟

在特权 EXEC 模式下开始，借助以下操作，可以配置 HSRP 认证和时钟。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）进入接口配置模式，并且进入欲设置认证的 HSRP 接口。

```
Switch(config)# interface interface-id
```

（3）认证 string 输入一个字符串，在所有的 HSRP 信息中被传载。认证字符串可以是 8 个字符的长度，默认的字符串是 cisco。

```
Switch(config)# standby[group-nuber]authentication string
```

（4）在其他路由器声明活动路由器 Down 掉之前，配置 hello 包和时间之间的时钟。

```
Switch(config)# standby[group-number]timers hellotime holdtime
```

（5）返回特权 EXEC 模式。

```
Switch(config)# end
```

（6）校验配置。

```
Switch# show running-config
```

（7）保存配置。

```
Switch(config)# copy running-config startup-config
```

使用 no standby [group-number] authentication string 接口配置命令去删除一个认证字符串。使用 no standby [group-number] timers hellotime holdtime 接口配置指令重新存储对于它们默认的时钟。

5. 配置 HSRP 组和簇

当一个设备正在参与一个 HSRP 备份路由器并且簇被启用时，可以为命令交换机冗余和 HSRP 冗余使用同一个备份组。使用 cluster standby-group HSRP-group-name [routing-redundancy]全局配置指令来为命令交换机和路由器冗余启用同一个 HSRP 备份组。如果创建一个带有同样 HSRP 备份组名称且没有 routing-redundancy 关键字的簇，HSRP 备份路由器对这个组就无效。

下面的例子就显示了怎么绑定备份组 my_hsrp 到簇，并且启用同一 HSRP 组命令交换机和路由器冗余。这个命令只在组命令交换机上被执行。如果备份组名称和号不存在，或者如果交换机是一个组员，就会出现错误信息。

```
Switch# configure terminal
Switch(config)# cluster standby-group my_hsrp routing-redundancy
Switch(config)# end
```

6. 显示 HSRP 配置

在特权 EXEC 模式下开始，使用下述命令显示 HSRP 的设置：

```
show standby[interface-id [group]] [brief] [detail]
```

如下所示为 2 个备份组(组 1 和组 100)的 HSRP 信息：

```
Switch# show standby
VLAN1-Group 1
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb
VLAN1-Group 100
Local state is Active, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 172.20.138.51 configured
Active router is local
Standby router is unknown expired
```

```
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

13.3.4 知识链接：链路汇聚和链路冗余技术

1. 链路汇聚技术

链路汇聚(Multi Link Trunk,MLT)技术是将网络设备的多个低带宽端口,捆绑成一条高带宽链路,从而实现链路负载平衡和相互冗余。汇聚后的链路容量是所有物理链路容量之和。如果其中一条物理链路中断时,整个逻辑链路不会中断,大大地提高了网络连接的可靠性。MLT 技术可以在多个不同网络设备间建立 MLT 连接,实现链路冗余。当一条链路出现故障时,可以将所有的数据流切换到另一个链路上,切换时间小于 1s,从而保证中心节点与骨干节点的可靠连接。

EtherChannel 和 Port Trunking 是最常用的交换机链路冗余技术。将交换机上多个物理端口同其他网络设备的多个端口连接起来,在逻辑上捆绑在一起,形成一个拥有较大带宽的"端口",用来充当网络中的干路传输,既可以增加交换机之间,以及交换机与服务器之间的连接带宽,实现均衡负载,又可提供链路冗余,如图 13-32 所示。Cisco 的 EtherChannel 有两个级别,即 Fast EtherChannel 和 Giga EtherChannel,最大带宽分别为 400Mbps 和 4Gbps。

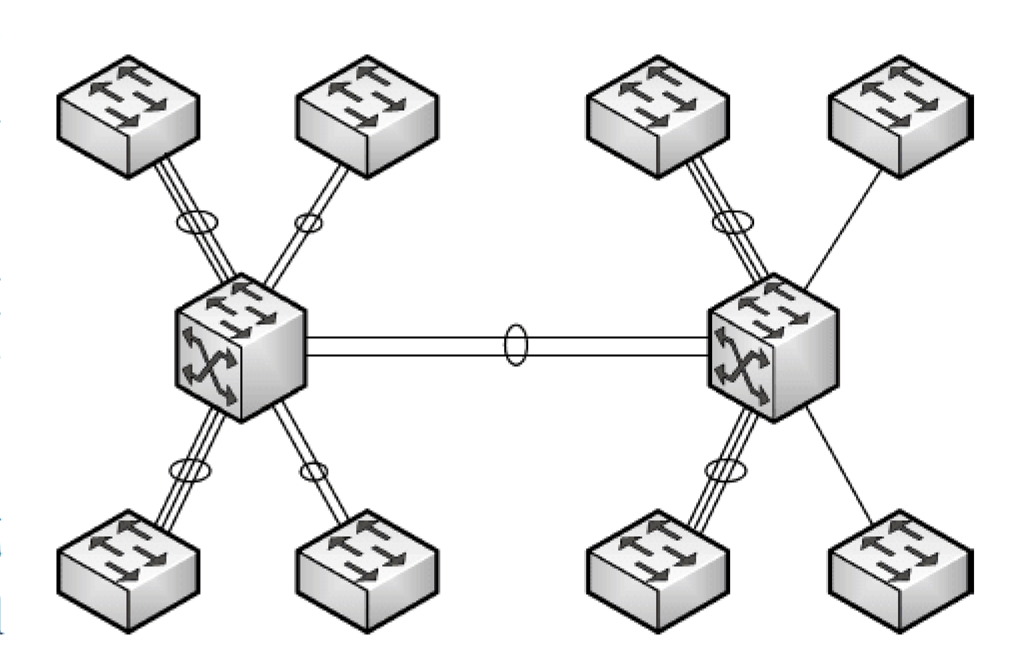


图 13-32 EtherChannel 冗余连接

Port Trunking 技术相对于 EtherChannel 技术实现起来更加简单,只需在支持 Trunking 功能的交换机上,将多个端口配置为一个逻辑端口,并将其配置为到某个 VLAN 连接即可。Port Trunking 管理非常灵活,不需要重新布线即可快速部署端口传输速率,同时也可以提供负载均衡能力以及系统容错功能。

注意：链路汇聚技术和端口汇聚技术可以将交换机之间、交换机和路由器之间的最多 4 条链路捆绑在一起,成倍增加网络传输带宽。通常情况下,配置 EtherChannel 的端口必须具备相同的属性,如双工模式、同为百兆或千兆端口、同为管理 VLAN 或拥有相同的 VLAN 边界、Trunking 状态等。配置 Trunking 时的端口有 Trunk、Auto、Desirable 等几种模式；配置 EtherChannel 时的端口有 Desirable、Auto、On 等几种模式。

2. 链路冗余技术

链路冗余也称链路备份,顾名思义,网络设备之间通过主链路和备份链路连接在一起,通常情况下都是主链路工作,只有当主链路无法正常工作时,备份链路自动接替主链路上的传输任务,从而保证网络传输的顺利进行。导致网络链路故障的原因有很多,除去设备或模块损坏等硬件故障原因以外,还可能由于瞬间网络流量过载、任务负荷过大而导致核心交换机瘫痪。因此,为了确保网络传输的可靠性必须为重要的网络设备连接创建冗余链路,如新交换机和骨干交换机之间,交换机和服务器之间等。

提示：链路冗余与负载均衡是两个概念,冗余往往与备份是联系在一起的,单纯有冗余

技术并不一定能实现负载均衡，而负载均衡技术是依赖于链路冗余的。

图 13-33 所示是汇聚交换机和核心交换机之间的链路冗余连接方式，事实上在这种拓扑结构的网络中会由于交换机之间的彼此连接而导致网桥循环（拓扑环），数据在交换机之间循环传递，并最终导致网络瘫痪。

借助交换机的扩展树（Spanning Tree）功能即可解决冗余链路中存在的拓扑环问题。Spanning Tree 实现冗余连接的工作方式是 Stand By（待机），即指定其中的主链路正常工作，而备份链路处于 Stand By 状态，并实时监控主链路的工作状态，一旦发生故障，立即开始工作。这种链路冗余方式，虽然不能提高网络传输速率，但可以充分保证网络链路的可靠性。

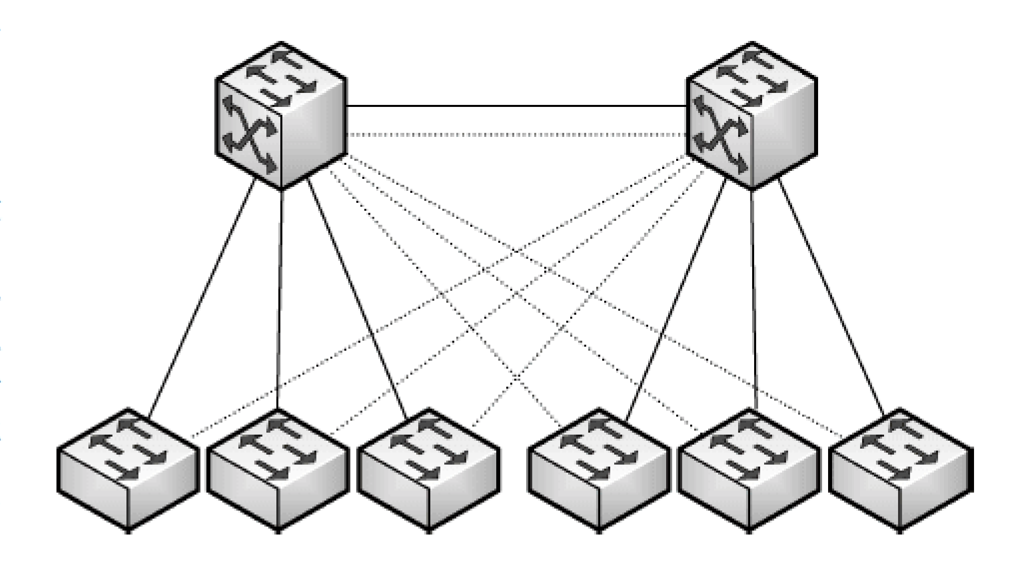


图 13-33　交换机之间的链路冗余

在启用 Spanning Tree 的交换机时，其接口处于以下几种状态之一。

（1）Blocking（阻塞），不参与帧的转发。

（2）Listening（侦听），当确定该接口将参与帧转发时，在阻塞状态后的第一个过渡状态。

（3）Learning（学习），准备参与帧转发。

（4）Forwarding（转发），转发帧。

（5）Disabled（禁用），端口处于 Shutdown 状态、没有连接，或者没有启用 Spanning Tree，从而不参与 Spanning Tree。

默认的 STP 配置参数如表 13-2 所示。

表 13-2　默认 STP 配置

特　　征	默 认 设 置
启用状态	VLAN 1 启用，最多可以启用 64 个 STP
交换机优先级	32768
STP 端口优先级	128
STP 端口费用	1000Mbps：4 100Mbps：19 10Mbps：100
STP VLAN 端口优先级	128
STP VLAN 端口费用	1000Mbps：4 100Mbps：19 10Mbps：100

默认状态下，所有 VLAN 中的扩展树都被启用。因此，无须为 VLAN 启用 STP，只需根据拓扑结构，确定根交换机，并调整端口费用和优先级值，从而设置最佳路径。

3. 路由冗余技术

单从核心交换机名称即可看出其在网络中的重要地位，几乎所有的跨网络访问都要经过这里，如果出现链路故障，则毫无疑问将导致网络瘫痪。借助路由热备份（Hot Stand by

Router Protocol，HSRP）和虚拟路由冗余（Virtual Router Redundancy Protocol，VRRP）技术可以使核心交换机双汇聚交换机中的某台交换机出现故障时，迅速切换三层路由设备和虚拟网关，实现双线路的冗余备份，保证整网稳定性。

（1）HSRP 技术

HSRP 协议的设计目标是为特殊环境下的路由转发提供支持，如主路由器断开等，此时将自动启用备份路由器，以维持网络的正常连通。例如，当源主机不能确定其第一跳路由器的目的 IP 地址时，HSRP 协议可以保护第一跳路由器不出故障。HSRP 协议中含有多种路由器，对应一个虚拟路由器（或三层交换机）。

HSRP 协议的工作机制如图 13-34 所示，其中负责转发数据包的路由器称之为活动路由器（Active Router）。一旦活动路由器出现故障，HSRP 将激活备用路由器（Stand by Routers）取代主动路由器。实际上，HSRP 协议只是提供了一种决定使用活动路由器还是备用路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的默认网关地址。

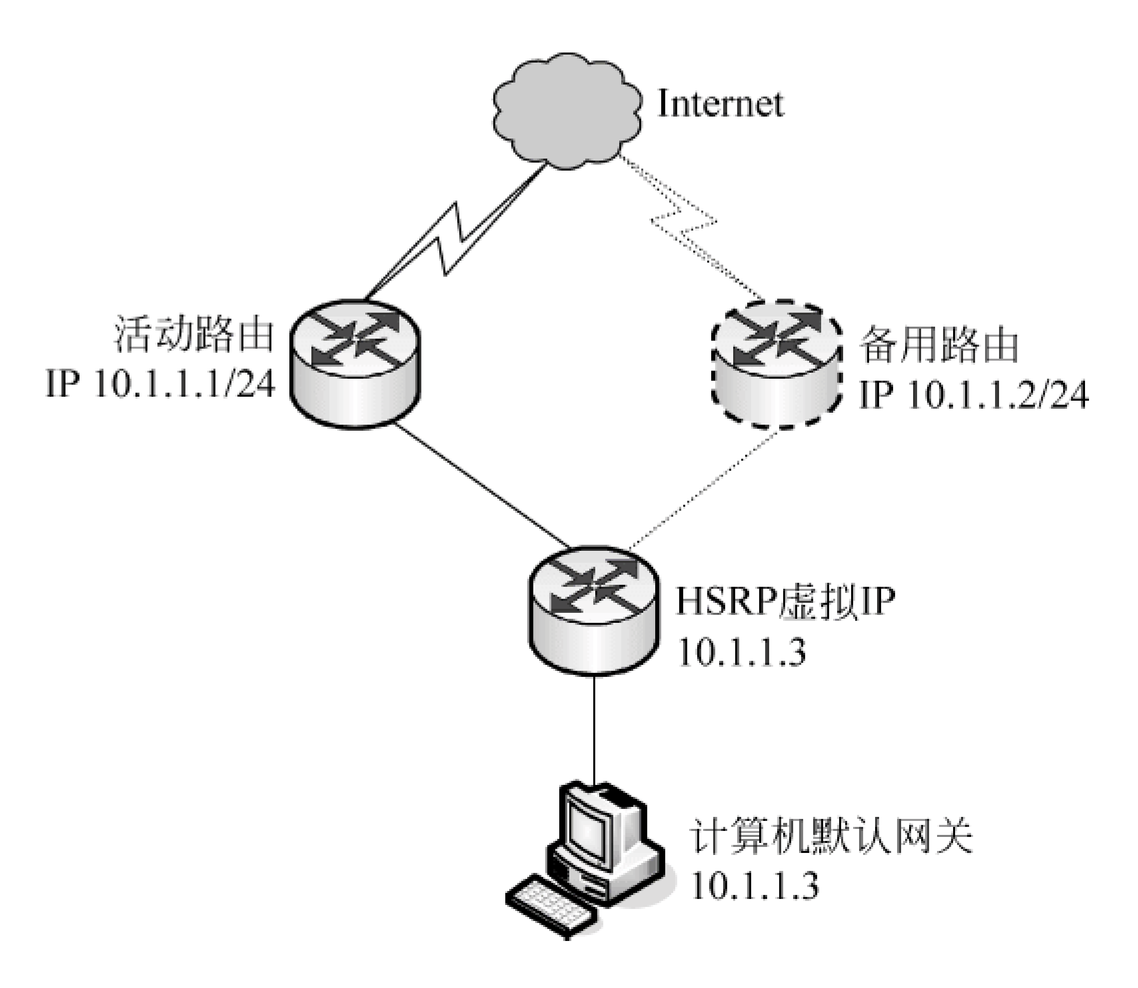


图 13-34　HSRP 工作过程

HSRP 的默认配置如表 13-3 所示。

表 13-3　HSRP 的默认配置

特　　性	默认设置
HSRP 组	未配置
备用组号	0
备用 MAC 地址	系统分配为：0000.0c07.acXX，XX 是 HSRP 组号
备用优先权	100
备用延迟	0（无延迟）
备用追踪接口优先权	10
备用 hello 时间	3s
备用 holdtime	10s

下面是配置 HSRP 的一些注意事项。

① HSRP 最多可以在 32 个 VLAN 或者路由器接口上配置。

② 在这个过程中，指定的接口必须在 3 层的接口中。

- 路由器端口。配置一个物理端口作为一个 3 层接口，输入 no switchport 接口配置命令。
- SVI。创建一个 VLAN 接口，使用 interface vlan vlan_id 全局配置指令，也可以使用 3 层默认接口。
- EtherChannel port channel in Layer 3 mode。使用 interface port-channel port-channel-number 全局配置命令和绑定以太网接口到 channel 组来创建一个 port-channel 逻辑接口。

③ 所有的 3 层接口都必须分配 IP 地址。

（2）VRRP 技术

VRRP 路由冗余技术主要是通过配置路由器组，实现多路由器的冗余。一组 VRRP 路由器协同工作，构成一台虚拟路由器，对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。同一 VRRP 组的路由器有两种角色，即主控路由器和备份路由器。在一个 VRRP 组中有且只有一台主控路由器，一台或多台备份路由器。VRRP 协议使用选择策略选出一台作为主控，负责 ARP 相应和转发 IP 数据包，组中的其他路由器作为备份的角色处于待命状态。当主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主路由器，由于切换迅速且无须改变 IP 地址和 MAC 地址，所以，对网络用户而言一切都是透明的。VRRP 路由冗余技术的工作机制如图 13-35 所示。

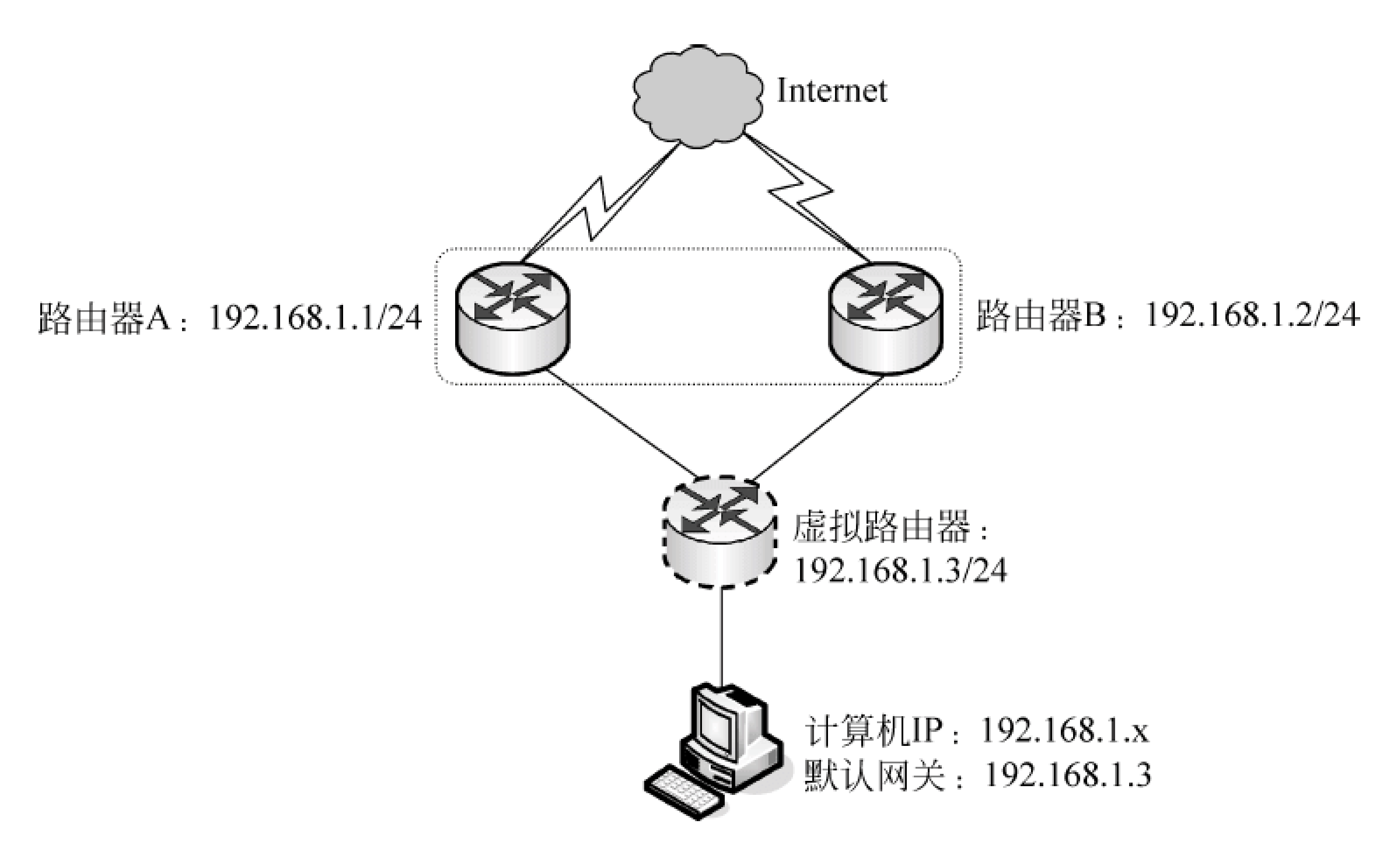


图 13-35　VRRP 工作机制

13.4　数据备份与恢复

在企业网络中，无论是 ERP 系统还是企业网站，得以稳定运行的根本都是对数据的访问和处理。数据的可靠性、可用性是衡量企业网络可靠性的重要依据，它直接决定企业业务是否能够顺利开展。数据的备份与恢复是保证信息系统安全可靠的基础，此处主要介绍网络中关键业务数据的备份，如域控制器、数据库等。

13.4.1 备份活动目录数据库

活动目录数据库的数据量虽然不像文件服务器那样巨大,但却十分重要,存储着网络上所有用户账户以及计算机等网络资源的信息,尤其是在单域控制器的网络中,其重要性更为突出。百密难免一疏,没有绝对安全的系统和硬件,最好的方法就是防患于未然。对于活动目录数据库而言,就是时刻做好备份工作,如果条件允许还可以多制作几份备份,提高安全性。万一发生严重故障,导致数据丢失或损坏,可以方便地从备份中还原该数据。

1. 安装 Windows Server Backup 组件

安装 Windows Server 2008 后,默认没有安装 Windows Server Backup 组件,需要管理员在“服务器管理器”的“功能”列表中,单独安装该组件。选择 Windows Server Backup 功能时,需要同时选择“Windows 恢复光盘”功能。

(1) 打开“服务器管理”窗口,依次选择“服务器管理器”→“功能”选项,显示“服务器管理器”窗口。单击“添加功能”链接,显示如图 13-36 所示的“选择功能”对话框。在“功能”列表中,展开 Windows Server Backup 功能,选中 Windows Server Backup 以及“命令行工具”复选框,显示“添加功能向导”对话框。提示将安装 Windows PowerShell 组件。单击“添加必需的功能”按钮,关闭“添加功能向导”对话框,返回到“选择功能”对话框。

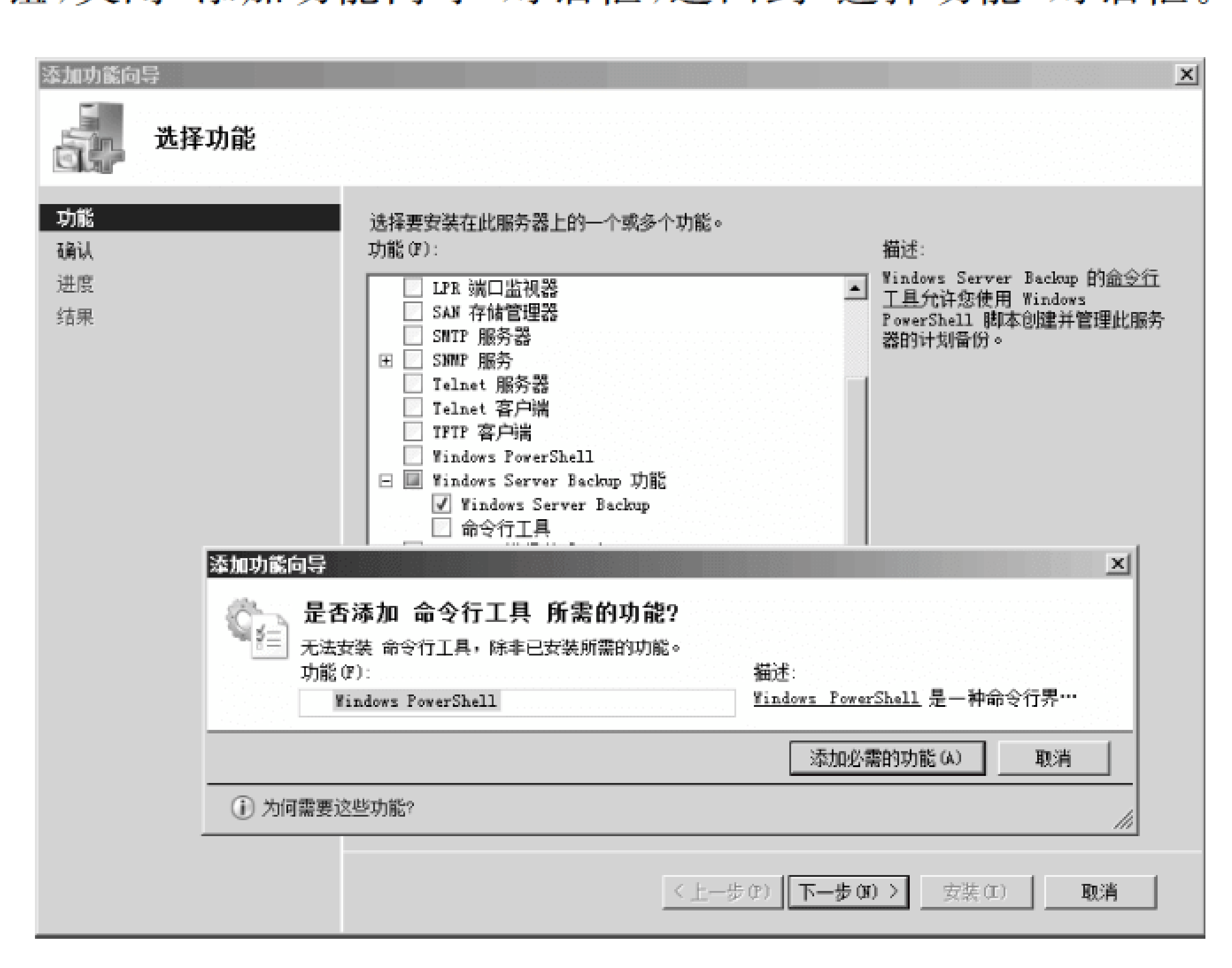


图 13-36 “选择功能”对话框

(2) 单击“下一步”按钮,显示“确认安装选择”对话框,显示需要安装的功能组件。单击“安装”按钮,安装备份功能必须的组件。安装完成后,单击“关闭”按钮,关闭“添加功能向导”,组件添加成功。

2. 创建服务器完整备份

在第一次备份 Active Directory 服务器时,建议使用完整备份的方法,在以后备份过程中,可以使用增量备份的方法。

(1) 打开“服务器管理”窗口,依次选择“服务器管理器”→“存储”→Windows Server Backup 选项,显示如图 13-37 所示的“服务器管理器”窗口。



图 13-37 “服务器管理器”窗口

(2) 在窗口右侧的“操作”面板中，单击“一次性备份”链接，启动“一次性备份向导”，显示如图 13-38 所示的“备份选项”对话框。如果是第一次使用一次性备份向导，建议选中“其他选项”单选按钮，为 Windows Server 2008 创建完整备份。

(3) 单击“下一步”按钮，显示如图 13-39 所示的“选择备份配置”对话框。如果选中“整个服务器(推荐)”单选按钮，则备份当前服务器所有磁盘；如果选中“自定义”单选按钮，允许管理员定制备份内容。

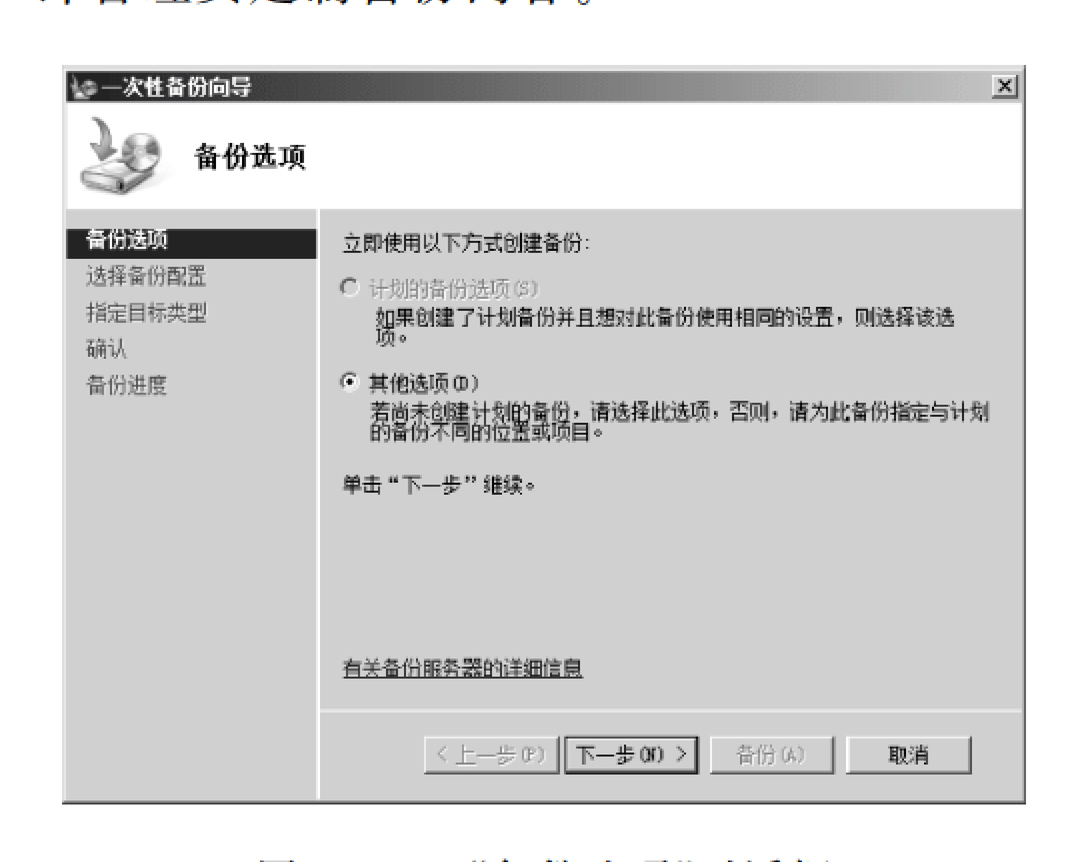


图 13-38 “备份选项”对话框

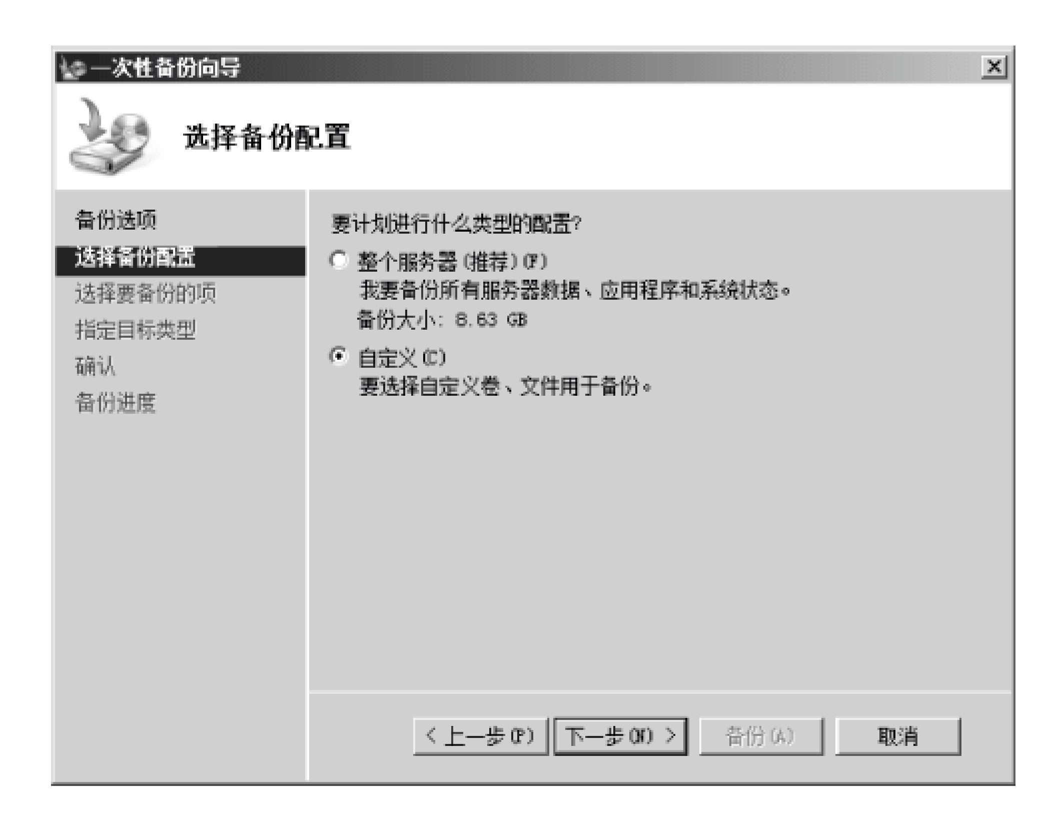


图 13-39 “选择备份配置”对话框

(4) 单击“下一步”按钮，显示如图 13-40 所示的“选择要备份的项”对话框。默认在备份列表中没有任何备份项目，需要管理员选择所要备份的项目。

(5) 单击“添加项”按钮，显示如图 13-41 所示的“选择项”对话框。在可备份列表中，选中所要备份的项目，这里选中“裸机恢复”复选框，此时会自动选中“系统状态”、“系统保留”和“本地磁盘(C:)”复选框。

(6) 单击“确定”按钮，返回“选择要备份的项”对话框。如果想要删除某备份项目，可以选中该项目，然后单击“删除项”按钮即可。单击“高级”按钮，显示如图 13-42 所示的“高级设置”对话框。单击“添加删除”按钮，添加所要删除的项目即可。

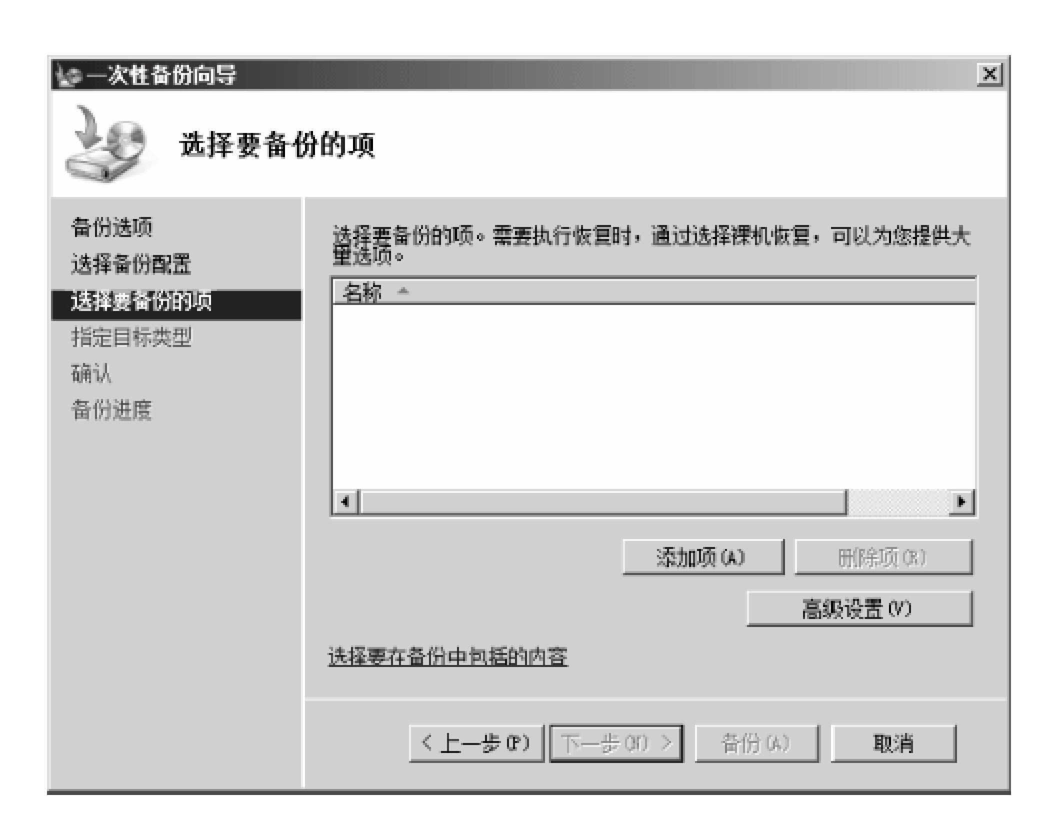


图 13-40 “选择要备份的项”对话框



图 13-41 “选择项”对话框

(7) 切换到如图 13-43 所示的“VSS 设置”选项卡，如果使用第三方的备份软件，建议选中“VSS 副本备份”单选按钮。如果使用 Windows Server 2008 提供的备份程序，建议选中“VSS 完整备份”单选按钮。



图 13-42 “高级设置”对话框



图 13-43 “VSS 设置”选项卡

(8) 单击“确定”按钮，返回“选择要备份的项”对话框，单击“下一步”按钮，显示如图 13-44 所示的“指定目标类型”对话框。一次性备份向导支持本地和网络 UNC 模式存储数据，同时支持本地 DVD 驱动器，可以将备份直接写到 DVD 备份设备中，这里选择目标类型为“本地驱动器”。

(9) 单击“下一步”按钮，显示如图 13-45 所示的“选择备份目标”对话框。选择用于备份的卷，在“备份目标”下拉列表框中，选择“本地磁盘(F)”选项。

(10) 单击“下一步”按钮，显示如图 13-46 所示的“确认”对话框，显示备份设置参数。

(11) 单击“备份”按钮，开始执行 Windows Server 2008 系统备份，显示如图 13-47 所示的“备份进度”对话框。

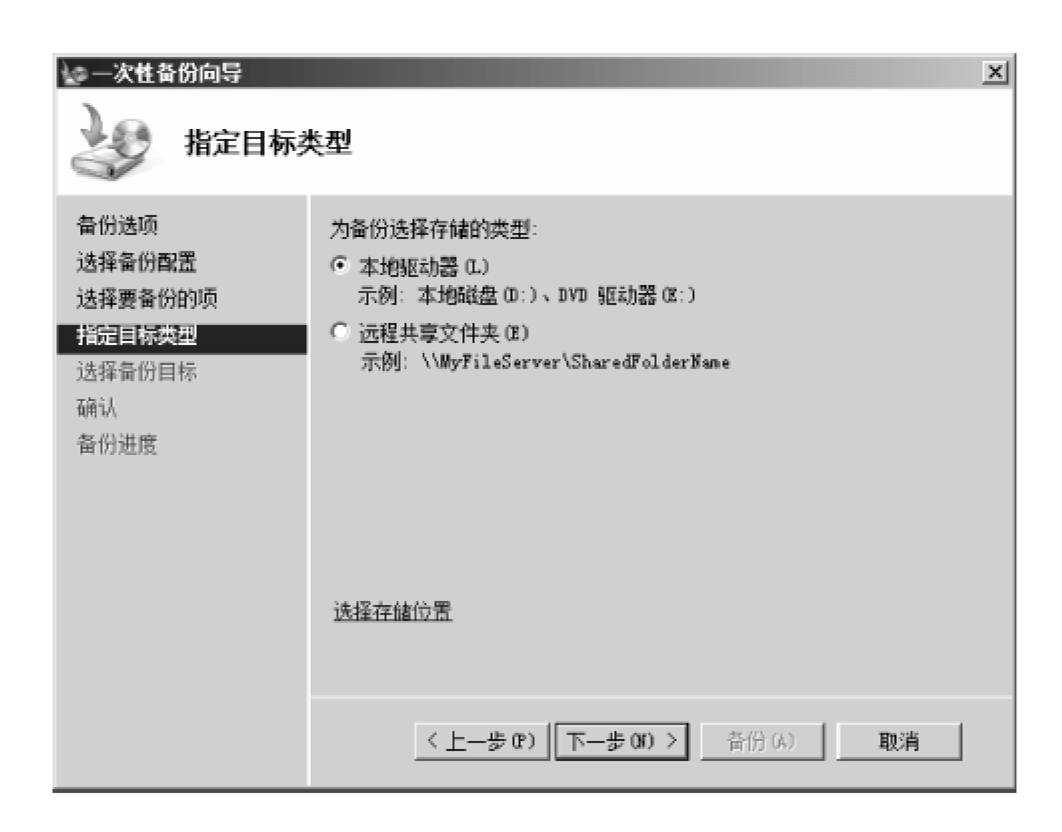


图 13-44　“指定目标类型”对话框



图 13-45　“选择备份目标”对话框

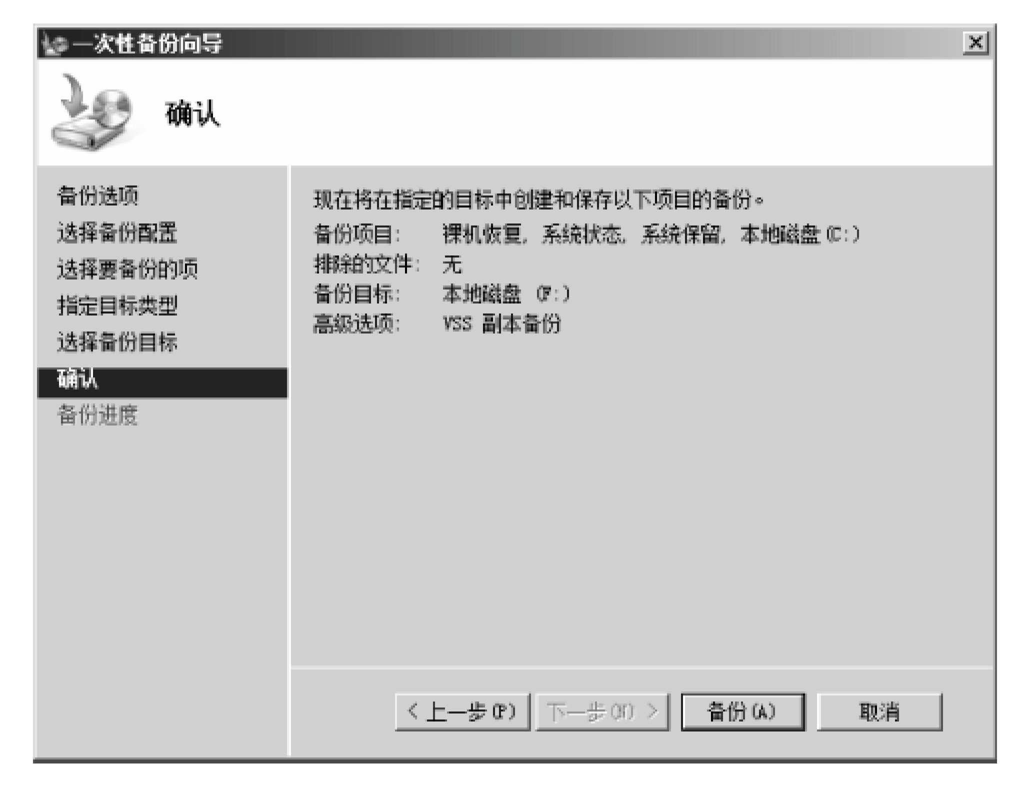


图 13-46　“确认”对话框



图 13-47　“备份进度”对话框

（12）单击“关闭”按钮，关闭一次性备份向导，备份过程在后台执行，管理员可以在“服务器管理器”中查看备份进程，如图 13-48 所示。



图 13-48　备份进程

(13) 备份完成后,在“服务器管理器”窗口显示备份成功信息。

3. 制定备份计划

Windows Server 2008 操作系统提供计划备份向导,帮助管理员自动完成某些备份任务,实现备份自动化。

(1) 打开 Windows Server Backup 窗口,在窗口右侧的“操作”面板中,单击“备份计划”链接,启动备份计划向导,直接单击“下一步”按钮,显示如图 13-49 所示的“选择备份配置”对话框,选择需要备份的设备类型,这里选中“自定义”单选按钮。

(2) 单击“下一步”按钮,显示如图 13-50 所示的“选择要备份的项”对话框。选择需要备份的目标项目,具体设置内容同“一次性备份”的操作,这里就不再赘述。



图 13-49 “选择备份配置”对话框

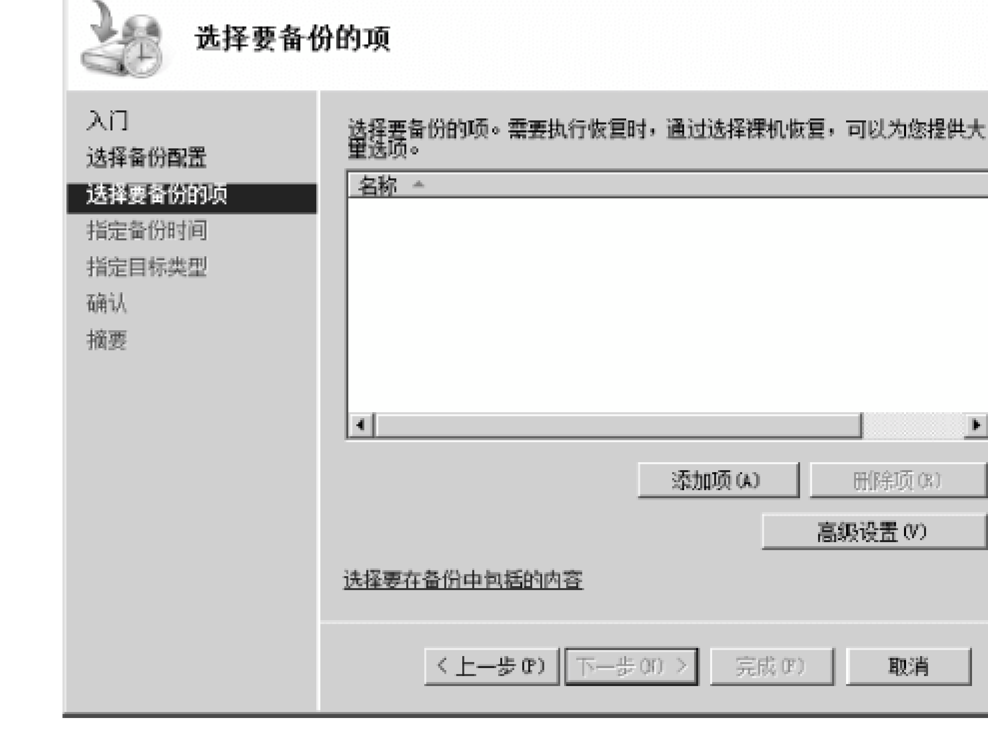


图 13-50 “选择要备份的项”对话框

(3) 单击“下一步”按钮,显示如图 13-51 所示的“指定备份时间”对话框,设置备份计划的执行周期。计划提供每日一次和每日多次两种模式。每日一次每天仅执行一次制定的备份,每日多次在每天的不同时刻执行多次系统备份。选中“每天多次”单选按钮,在“可用时间”列表中,选择需要执行备份的时间。单击“添加”按钮,将选择的时间添加到“已计划的时间”列表中。重复操作,设置备份周期。

(4) 单击“下一步”按钮,显示如图 13-52 所示的“指定目标类型”对话框,根据需要选择所要备份到的目标位置。

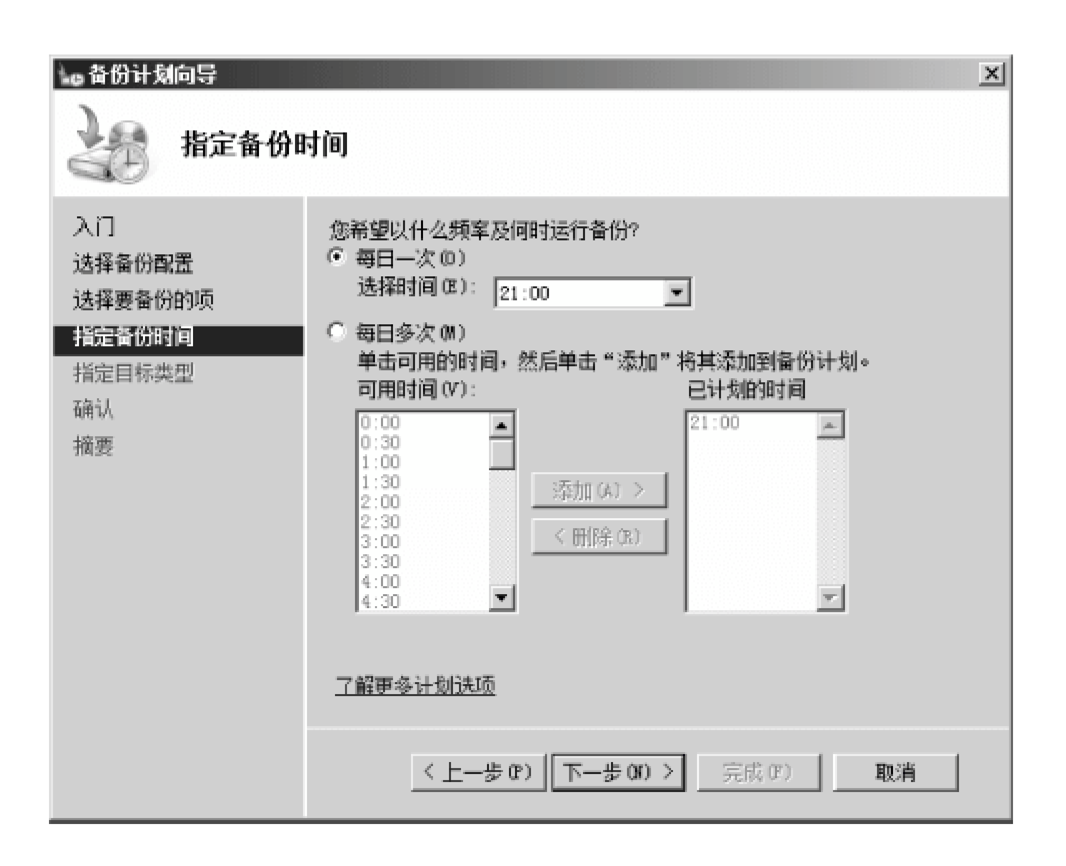


图 13-51 “指定备份时间”对话框

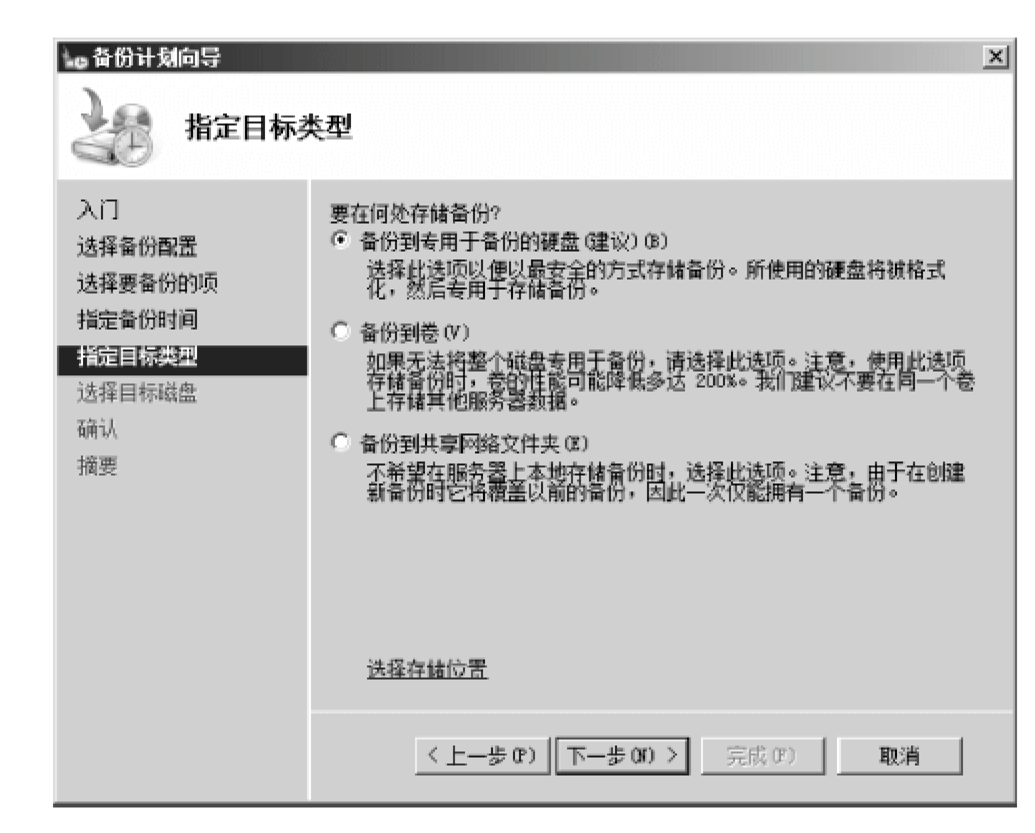


图 13-52 “指定目标类型”对话框

① 备份到专用于备份的磁盘：使用专用的磁盘作为备份磁盘。需要注意的是，如果选择该选项，在设置磁盘后，会对磁盘进行格式化。

② 备份到卷：将数据备份到当前系统的卷中。

③ 备份到共享网络文件夹：将数据备份到网络中的其他共享网络文件夹中。

（5）单击“下一步”按钮，显示如图13-53所示的“选择目标磁盘”对话框。单击“显示所有可用磁盘”按钮，打开“显示所有可用磁盘”对话框，在“可用磁盘”列表中，选择所要备份的目标磁盘。



图13-53　“选择目标磁盘”对话框

（6）单击“确定”按钮，返回“选择目标磁盘”对话框，并选中磁盘前面的复选框。单击“下一步”按钮，显示如图13-54所示的Windows Server Backup对话框。向导完成后，将格式化所选择的磁盘，并且在Windows资源管理器中，将不显示作为备份设备的磁盘。

（7）单击“是”按钮，显示如图13-55所示的“确认”对话框，显示备份计划设置参数。

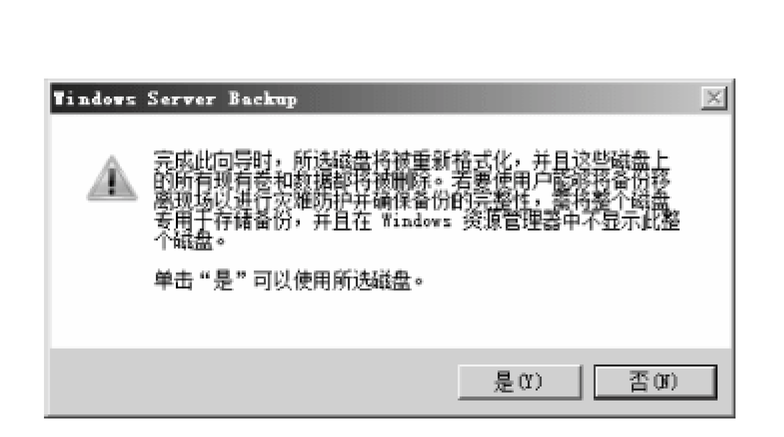


图13-54　Windows Server Backup对话框



图13-55　“确认”对话框

（8）单击“完成”按钮，显示如图 13-56 所示的“摘要”对话框，在此过程中将格式化目标磁盘以及创建备份计划。



图 13-56　“摘要”对话框

（9）单击“关闭”按钮，关闭“备份计划”向导，完成备份计划的创建。

13.4.2　还原活动目录数据库

域控制器的数据库损坏或数据丢失，将直接影响到网络功能的提供，尤其是在单域网络环境中，活动目录数据库的备份显得更为重要。如果仅是数据库故障，则直接使用备份文件恢复数据库即可。需要注意的是，活动目录数据库的恢复，需要在“目录服务还原模式”下完成，主要操作步骤如下。

（1）在启动域控制器时，按 F8 键启动到“高级启动选项”画面，如图 13-57 所示。需要注意的是，只有安装 Windows Server Backup 中的命令行工具后，启动菜单中才会出现“目录服务还原模式”。

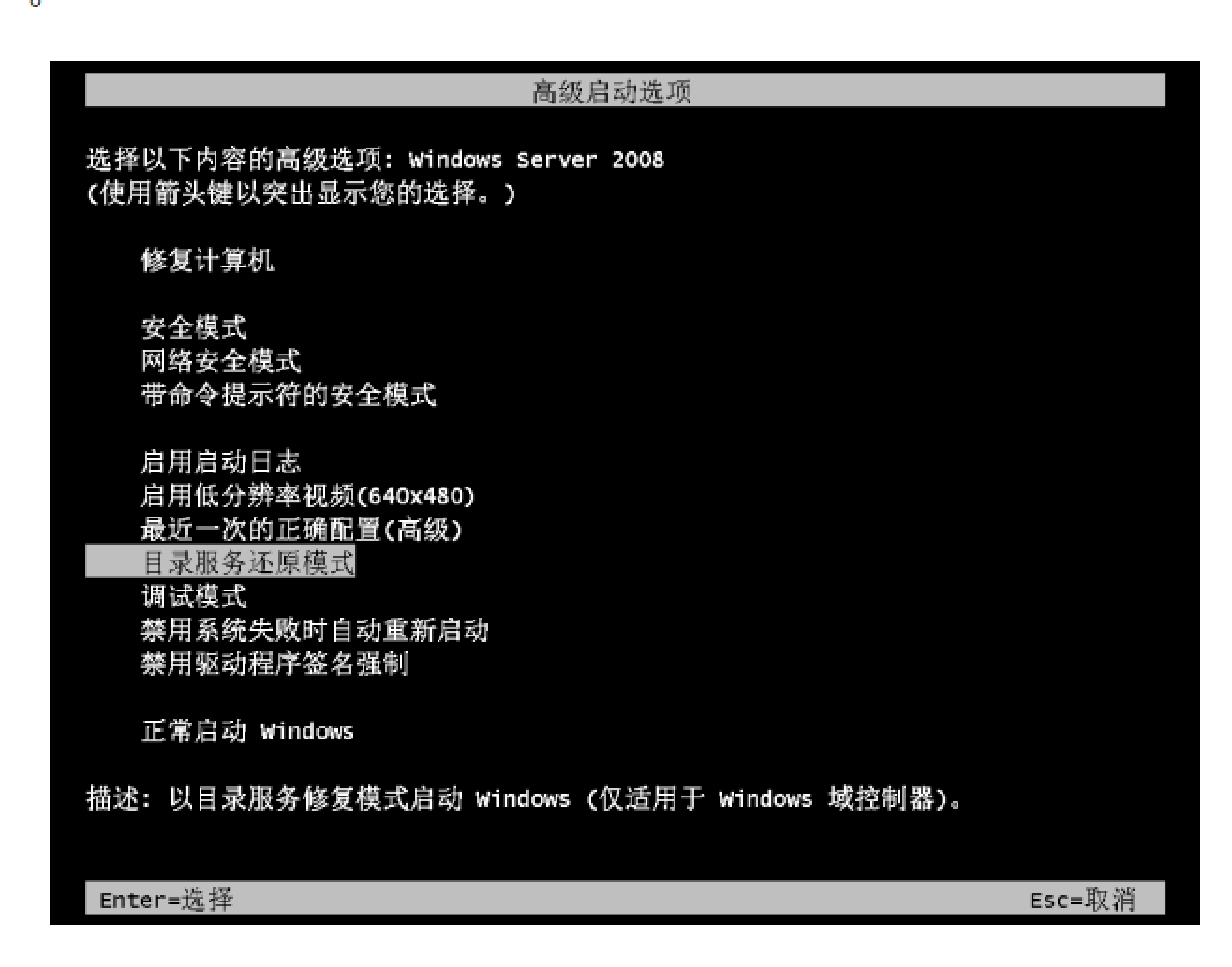


图 13-57　“高级启动选项”画面

(2) 选择“目录服务还原模式”并按 Enter 键,开始启动系统。需要注意的是,必须以本地系统管理员账户登录系统,如图 13-58 所示。此时的域控制器是不可用的。

(3) 启动到 Windows 安全模式后,打开“命令提示符”窗口,输入如下命令:

```
wbadmin get versions
```

按 Enter 键,显示如图 13-59 所示的结果。恢复目录数据库时是通过每次备份的版本信息确定的,默认格式为:mm/dd/yyyy-hh:mm,如 06/01/2008-08:49。



图 13-58 登录系统



图 13-59 查看备份版本标识

(4) 继续输入如下命令:

```
wbadmin start systemstaterecovery-version: 09/14/2009-08:29
```

按 Enter 键运行,提示网络管理员是否要执行系统状态恢复。

(5) 根据提示输入 Y 并按 Enter 键,确认要执行系统状态恢复,提示网络管理员使用的复制引擎类型。如果复制引擎类型不同,系统状态将不能正确恢复。

(6) 恢复完成后,提示用户需要重新启动计算机才能使恢复生效。需要注意的是,由于被恢复的系统文件比较多,重新启动服务器可能需要较长的时间。

(7) 重新启动完成后,提示系统状态已经成功恢复,按 Enter 键继续即可。

活动目录数据库的恢复需要一个良好的备份,即备份时间离当前时间不超过系统默认的时间限制。当活动目录中的一个对象被删除时,并不是彻底地消失。事实上,这时的对象成为一个临时被标记为“墓碑”的记录。一定时间之后,系统才会将标记为“墓碑”的记录永久删除。因此,在“墓碑”记录被删除之前,管理员仍然可以通过数据库备份恢复被删除用户的账户信息。对于超过时间限制的备份,即使能够恢复,域中的客户端信息也将失去同步功能,彼此之间的安全通道将被破坏。

提示:*在 Windows Server 2003 系统中“墓碑”记录的默认保留时间为 60 天,而在 Windows Server 2008 和 Windows Server 2003 SP1 系统中默认为 180 天。若想恢复任意时间的活动目录数据库备份,必须将“墓碑”记录保留足够长的时间。*

(1) 依次选择“开始”→“管理工具”→ADSI Edit 选项,打开“ADSI Edit”窗口。Active Directory 服务界面编辑器(ADSI 编辑)是一个轻型目录访问协议(LDAP)编辑器,类似于组策略编辑器和注册表编辑器,可用来管理 Active Directory 域服务中的对象和属性。

（2）右击 ADSI Edit 并在快捷菜单中选择“连接到”选项，显示如图 13-60 所示的“连接设置”对话框。在“连接点”选项区中，选中“选择一个已知命名上下文”单选按钮，并选择下拉列表框中的“配置”选项。在“计算机”选项区中，系统默认选中“默认(您登录到的域或服务器)”单选按钮，如果需要连接其他服务器，则可以选中“选择或键入域或服务器”单选按钮，选择服务器并指定通信端口。



图 13-60 “连接设置”对话框

（3）单击“确定”按钮，返回 ADSI Edit 窗口。依次展开“配置[AD1.coolpen.net]”→CN=Configuration，DC=coolpen，DC=net→CN=Services→CN=Windows NT→CN=Directory Service 选项。右击 CN=Directory Service，选择快捷菜单中的“属性”选项，显示如图 13-61 所示的“CN=Directory Service 属性”对话框。

（4）选中 TombstoneLifetime 并单击“编辑”按钮，显示如图 13-62 所示的“整数属性编辑器”对话框。在“值”文本框中，输入新的“墓碑”生存时间即可，如 3600，默认时间单位为天。

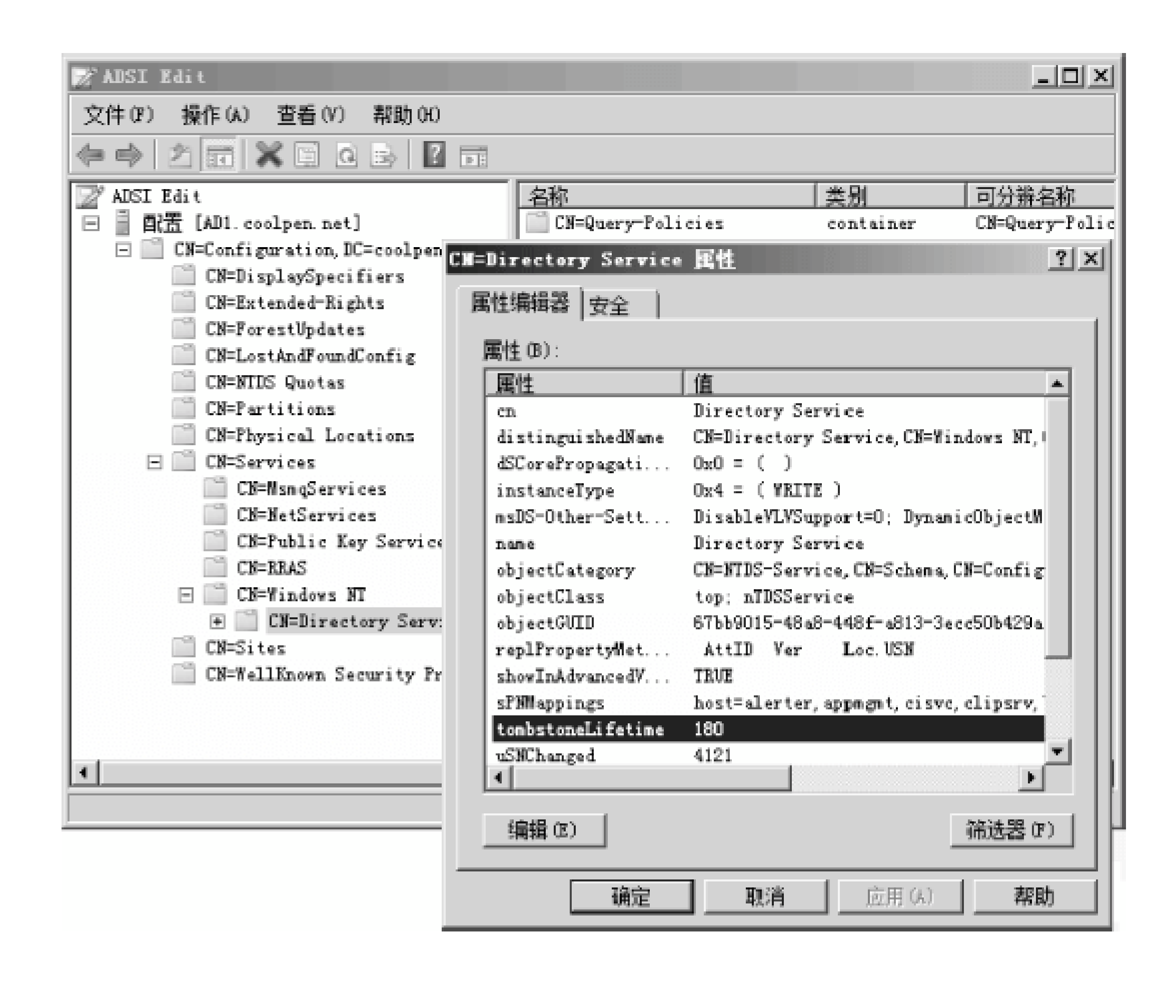




图 13-61 “CN=Directory Service 属性”对话框　　图 13-62 “整数属性编辑器”对话框

（5）连续单击“确定”按钮保存设置，完成墓碑生存时间的修改。

13.4.3　备份 SQL Server 数据库

目前，该企业网络中使用的数据库服务器是 Microsoft 的 SQL Server 2005。SQL Server 支持多种备份机制。完全备份/恢复数据库，是网络管理员必须掌握数据安全保护技术。如果数据量不是很大的业务应用，建议网络管理员经常完全备份数据库。

1．完全备份数据库

完全备份数据库就是将数据库中所有数据文件全部复制，包括完全数据库备份过程中数据库的所有行为。所有用户数据以及所有数据库对象，包括系统表、索引和用户自定义表。对于小型数据库，这种方法是可行的。但对于中型或者大型的数据库，这种备份方式需要花费较多的备份时间以及存储空间。

（1）在 SQL Server Management Studio 控制台中，选择希望备份的数据库对象，例如 ReportServerTempDB，右击 ReportServerTempDB，依次选择“任务”→“备份”选项，显示如图 13-63 所示的“备份数据库-ReportServerTempDB”对话框。在“源”选项区域中，选择“备份类型”下拉列表框中的“完整”，在“备份组件”选项区域中选中“数据库”单选按钮。在“备份集”选项区域中，指定备份集的相关信息，包括“名称”、“说明”和“备份集过期时间”。如果设置过期时间的值为 0，则表示始终不过期。在“目标”选项区域中，选择保存数据库备份的目标路径。如果服务器上安装了磁带设备，则磁带选项可选。

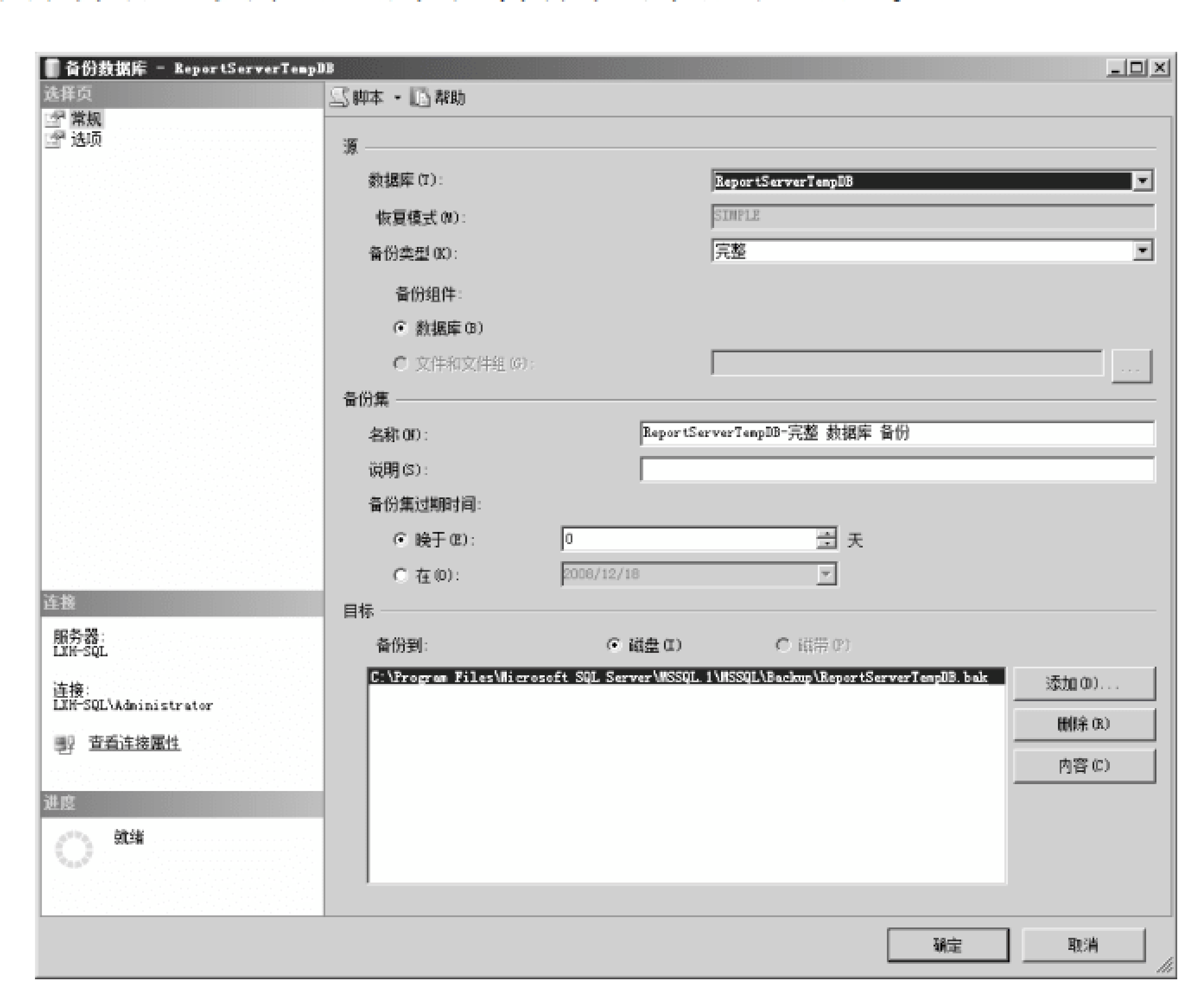


图 13-63　“备份数据库-ReportServerTempDB”对话框

（2）单击“添加”按钮，显示如图 13-64 所示的“选择备份目标”对话框。在“文件名”编辑框中，输入数据库备份文件存放的目标文件夹。

（3）单击“…”按钮，显示如图 13-65 所示的“定位数据库文件”对话框，选择备份数据的路径，例如 D:\，根据实际情况在“文件名”文本框中输入文件名称，例如 ReportservertempDB-081219。在“文件类型”下拉列表框中，保持默认设置即可。

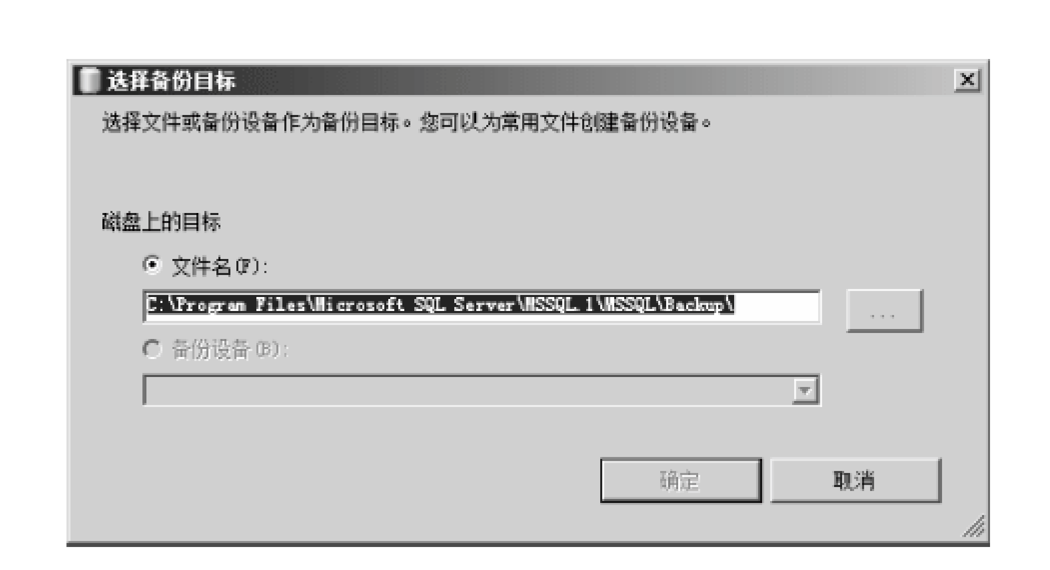




图 13-64 “选择备份目标”对话框

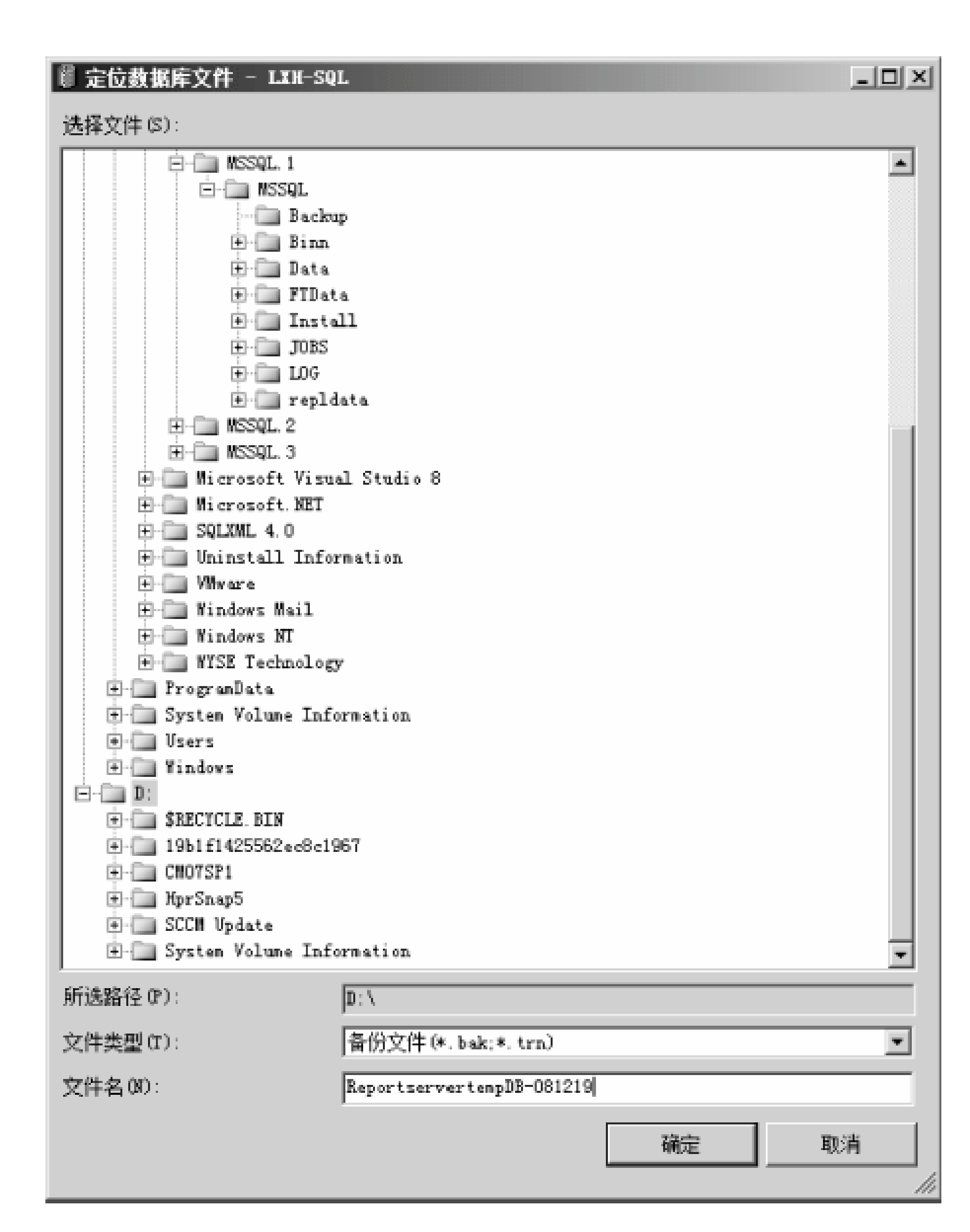


图 13-65 “定位数据库文件”对话框

(4) 连续单击“确定”按钮，返回到“备份数据库-ReportServerTempDB”对话框，删除默认的保存备份路径，设置完成的参数如图 13-66 所示。

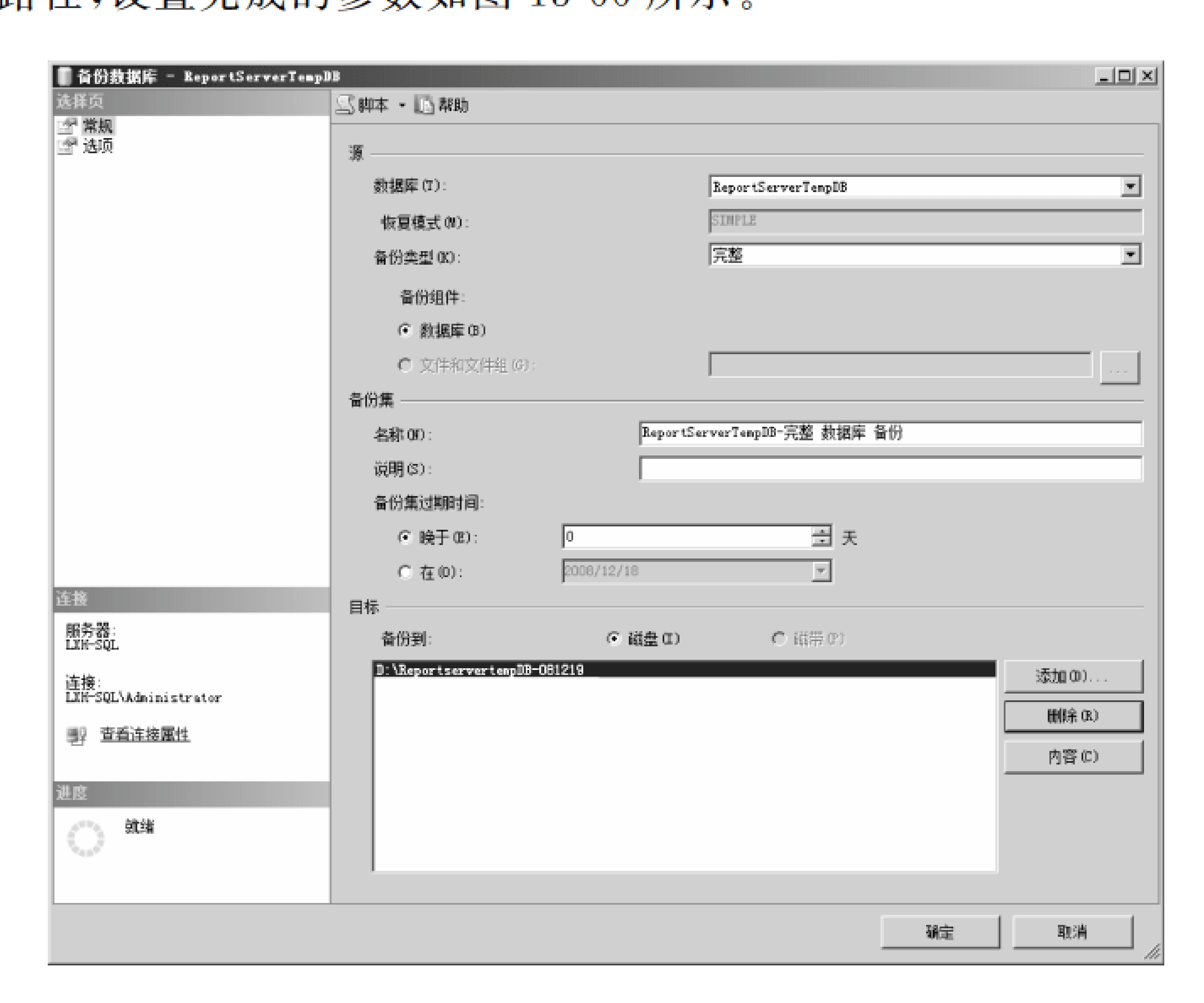


图 13-66 “备份数据库-ReportServerTempDB”对话框

(5) 单击“确定”按钮，开始执行数据库备份。数据库备份完成后，显示如图 13-67 所示的 Microsoft SQL Server Management Studio 对话框。

2. 创建自动备份数据库计划

Microsoft SQL Server 2005 数据库提供了备份策略，可以帮助网络管理员完成数据库



图 13-67 Microsoft SQL Server Management Studio 对话框

和事务日志的自动备份，同时可以完成数据库和事务日志的完整性自动验证。这里将通过 Microsoft SQL Server 2005 的维护计划向导，建立数据库和事务日志的自动备份策略，策略内容如下：每天 00:30:00 完整备份数据库，每天每小时自动备份事务日志。

(1) 在 Microsoft SQL Server Management Studio 控制台中，依次展开 LXH-SQL→"管理"→"维护计划"选项，如图 13-68 所示。

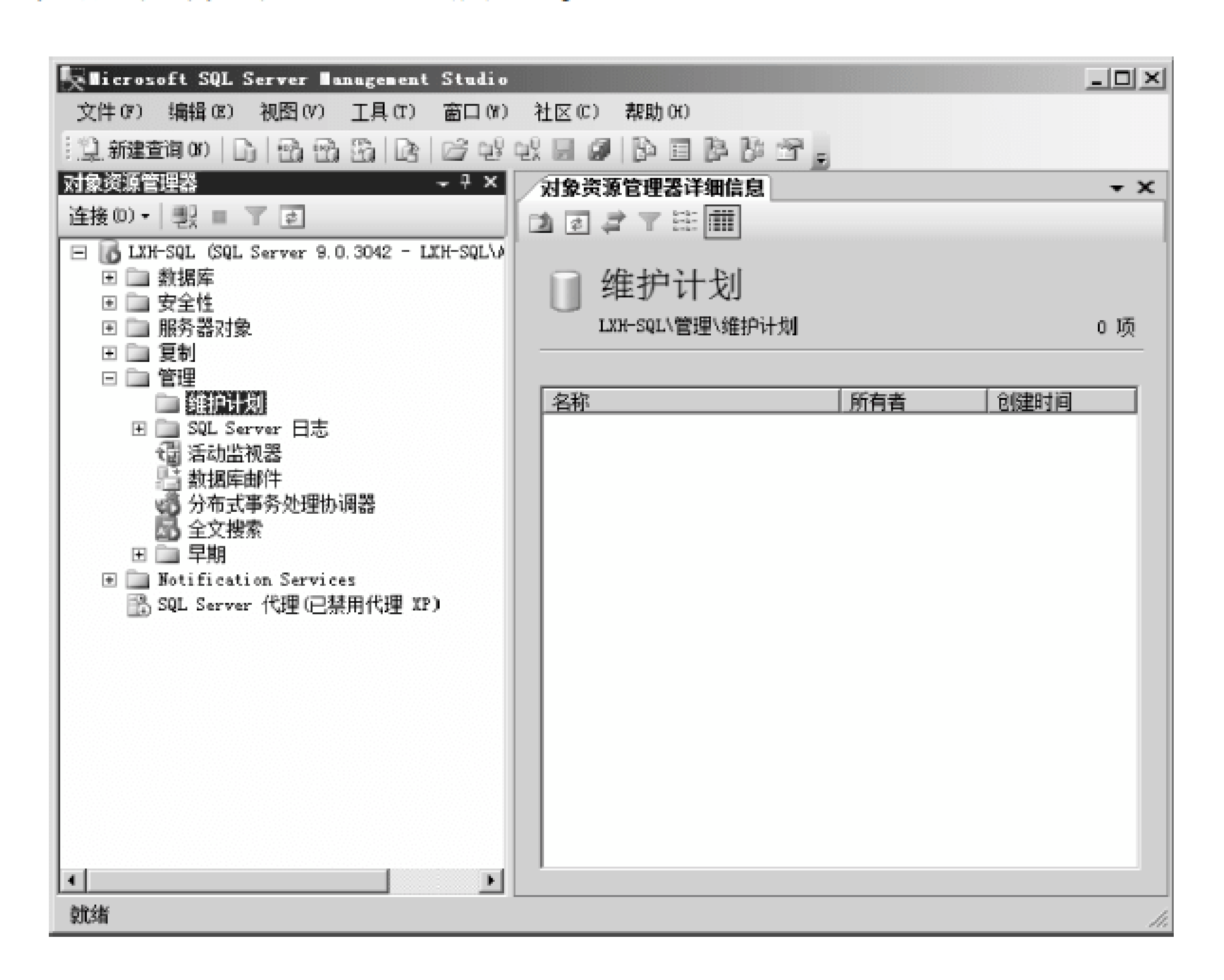


图 13-68 "维护计划"窗口

(2) 右击"维护计划"，在快捷菜单中选择"维护计划向导"选项，启动维护计划向导，显示如图 13-69 所示的"SQL Server 维护计划向导"对话框。

注意：执行此操作前，必须确保已经启用"SQL Server 代理"服务，否则将无法启动维护计划向导。

(3) 单击"下一步"按钮，显示如图 13-70 所示的"选择计划属性"对话框，在"名称"文本框中，输入当前计划的名称，也可以使用默认名称，并选中"整个计划统筹安排或无计划"单选按钮。

(4) 单击"更改"按钮，显示如图 13-71 所示的"作业计划属性-MaintenancePlan"对话框。在"计划类型"下拉列表框中，选择计划类型为"重复执行"选项，选中"已启用"复选框。在"频率"选项区域中，选择作业的执行方式为"每天"选项，即每天执行数据库备份计划。执行间隔为"1"天。在"每天频率"选项区域中，选中"执行一次，时间为："单选按钮，每天数据库备份的开始时间为"00:30:00"。在"持续时间"选项区域中，默认"开始日期"是该作业的创建日期；默认"结束日期"是选择"无结束日期"，除非网络管理员手动停止该作业，否则该作业将持续执行。设置完成后，单击"确定"按钮，返回"选择计划属性"对话框。



图 13-69 “SQL Server 维护计划向导”对话框



图 13-70 “选择计划属性”对话框

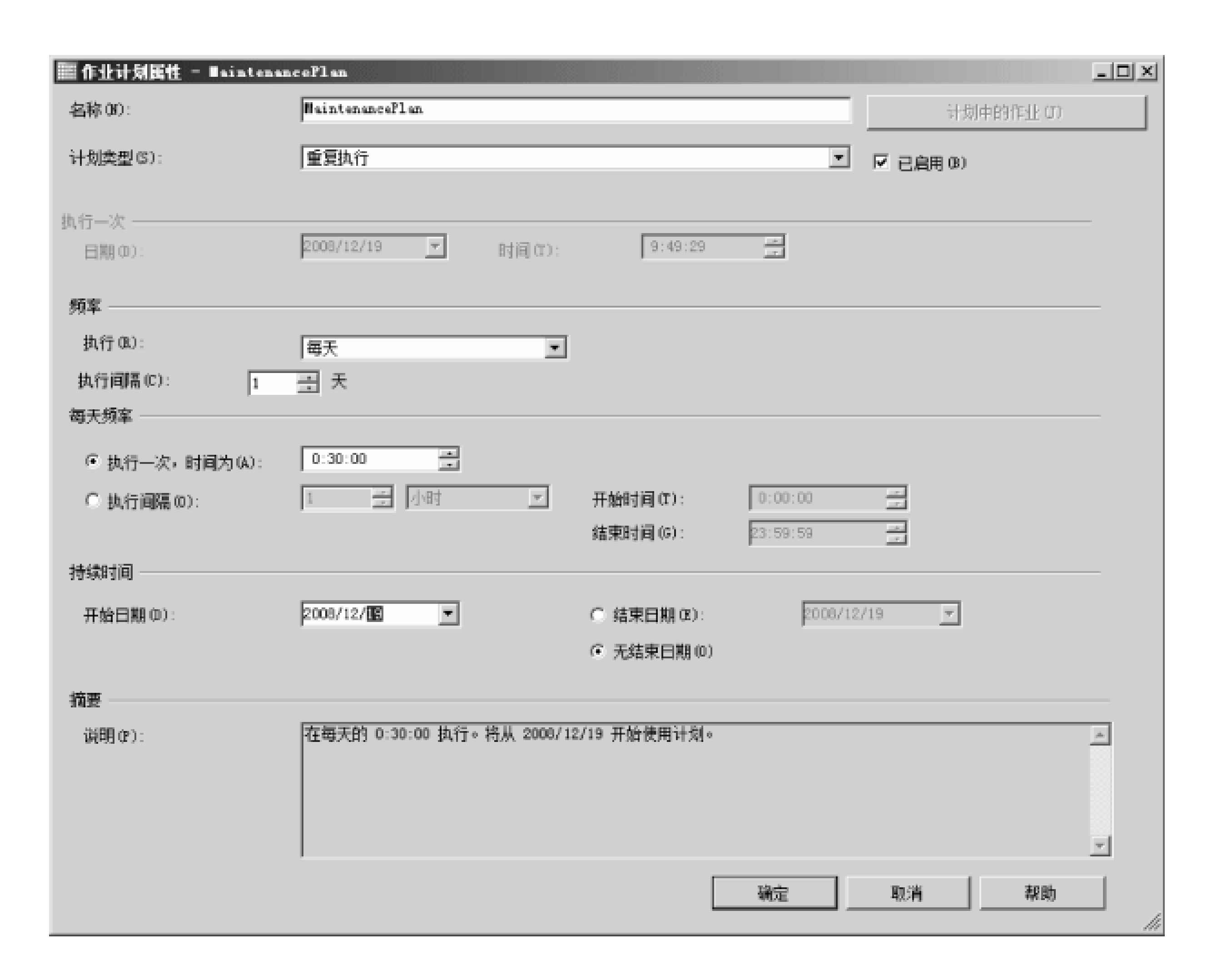


图 13-71 “作业计划属性-MaintenancePlan”对话框

提示：网络管理员根据实际情况调整“作业计划”的执行时间，以及执行的频率、间隔时间。

(5) 单击“下一步”按钮，显示如图 13-72 所示的“选择维护任务”对话框。在“选择一项或多项维护任务”下拉列表框中，选择维护任务，例如，选中“备份数据库(完整)”维护任务。此时，可以在下方文本框中查看所选维护任务的描述信息。

(6) 单击“下一步”按钮，显示如图 13-73 所示的“选择维护任务顺序”对话框。如果在“选择执行任务的顺序”列表中，包含多个维护任务，选择需要调整顺序的维护任务，单击“上移”或者“下移”按钮，即可调整维护任务的执行顺序。

提示：数据库维护任务执行顺序有先后之分，在设置执行顺序的时候，需要确认维护任务的目的，然后调整执行的顺序。

(7) 单击“下一步”按钮，显示如图 13-74 所示的“定义‘备份数据库(完整)’任务”对话框，此时尚未选择维护任务的操作对象。

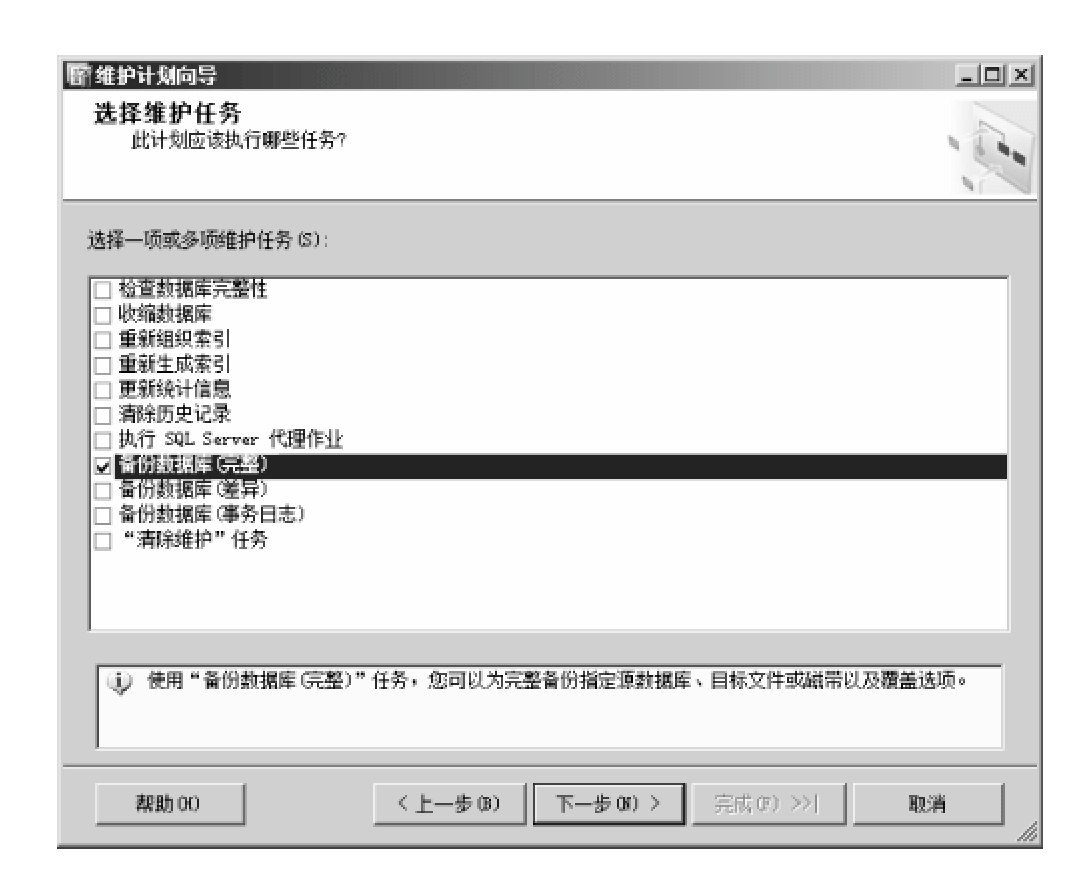


图 13-72 "选择维护任务"对话框

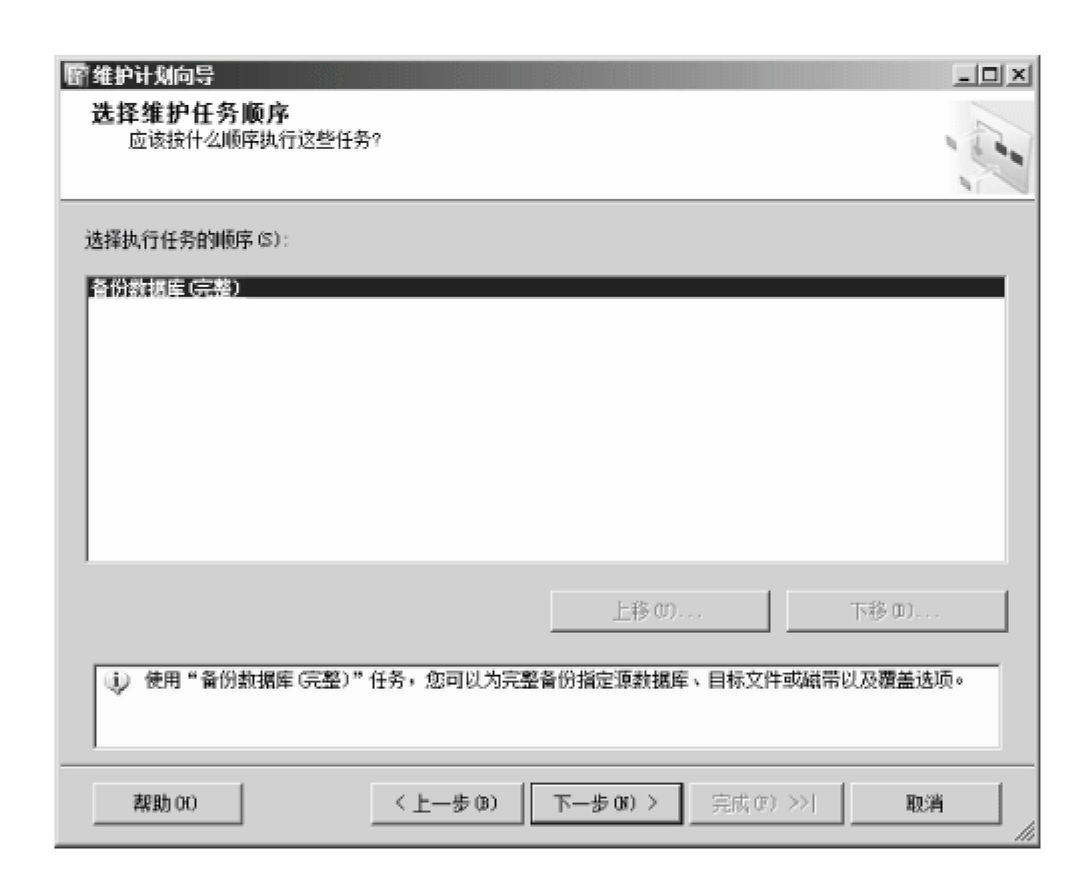


图 13-73 "选择维护任务顺序"对话框

(8) 单击"数据库"下拉按钮，显示如图 13-75 所示的数据库选择下拉列表框，选中"以下数据库"单选按钮，并指定希望执行计划任务的数据库对象，此处以 ReportServerTempDB 数据库为例。



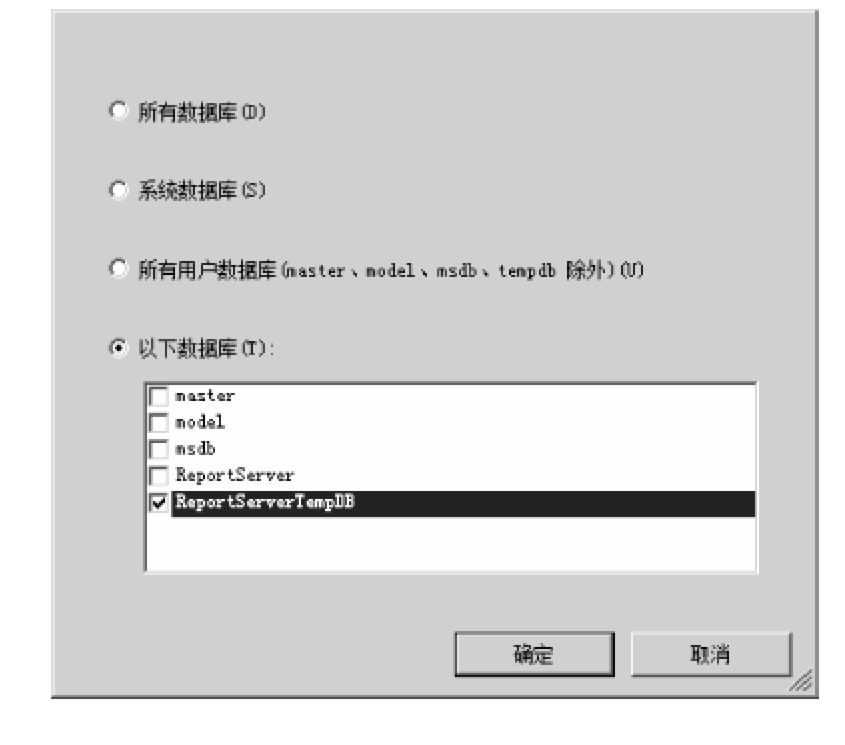


图 13-74 "定义'备份数据库(完整)'任务"对话框　　图 13-75 数据库下拉列表框

(9) 单击"确定"按钮，返回如图 13-76 所示的"定义'备份数据库(完整)'任务"对话框。此时，"数据库"的设置自动更新为"特定数据库"。该对话框中的配置选项与备份数据库时类似，主要包括设置备份过期时间、保存路径等，此处不再赘述。

(10) 单击"下一步"按钮，显示如图 13-77 所示的"选择报告选项"对话框，使用默认设置即可。

(11) 单击"下一步"按钮，显示如图 13-78 所示的"完成该向导"对话框。

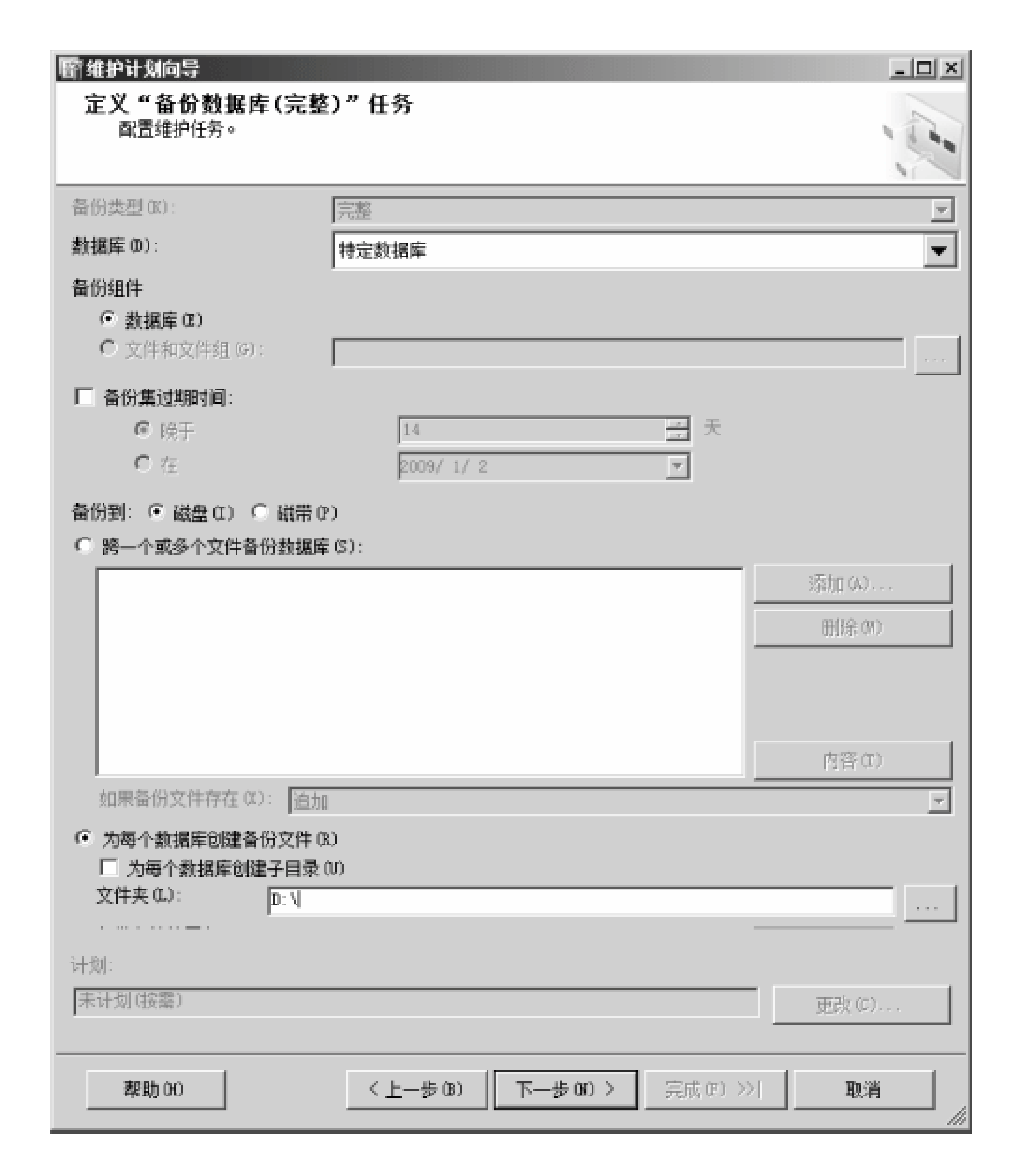




图 13-76 “定义‘备份数据库(完整)’任务”对话框

图 13-77 “选择报告选项”对话框

(12) 单击“完成”按钮，显示如图 13-79 所示的“维护计划向导进度”对话框。







图 13-78 “完成该向导”对话框

图 13-79 “维护计划向导进度”对话框

(13) 单击“关闭”按钮，关闭维护计划向导。

13.4.4 恢复 SQL Server 数据库

在恢复数据库前，必须确保已经为该数据库创建了备份。这里仍以 ReportServerTempDB 数据库为例，介绍如何恢复完全备份的数据库。

(1) 在 Microsoft SQL Server Management Studio 控制台中，选择想要恢复的数据库对象。右击数据库名，依次选择快捷菜单中的“任务”→“还原”→“数据库”选项，显示如图 13-80 所示的“还原数据库-ReportServerTempDB”对话框。在“还原的目标”选项区域中，设置“目标数据库”名称和“目标时间点”，系统默认的目标时间点为“最近状态”。已经备

份的数据库文件模式使用的是“完整”模式备份，因此使用默认值即可。在“还原的源”选项区域中，指定用于还原备份集的源和位置，选中“源设备”单选按钮。

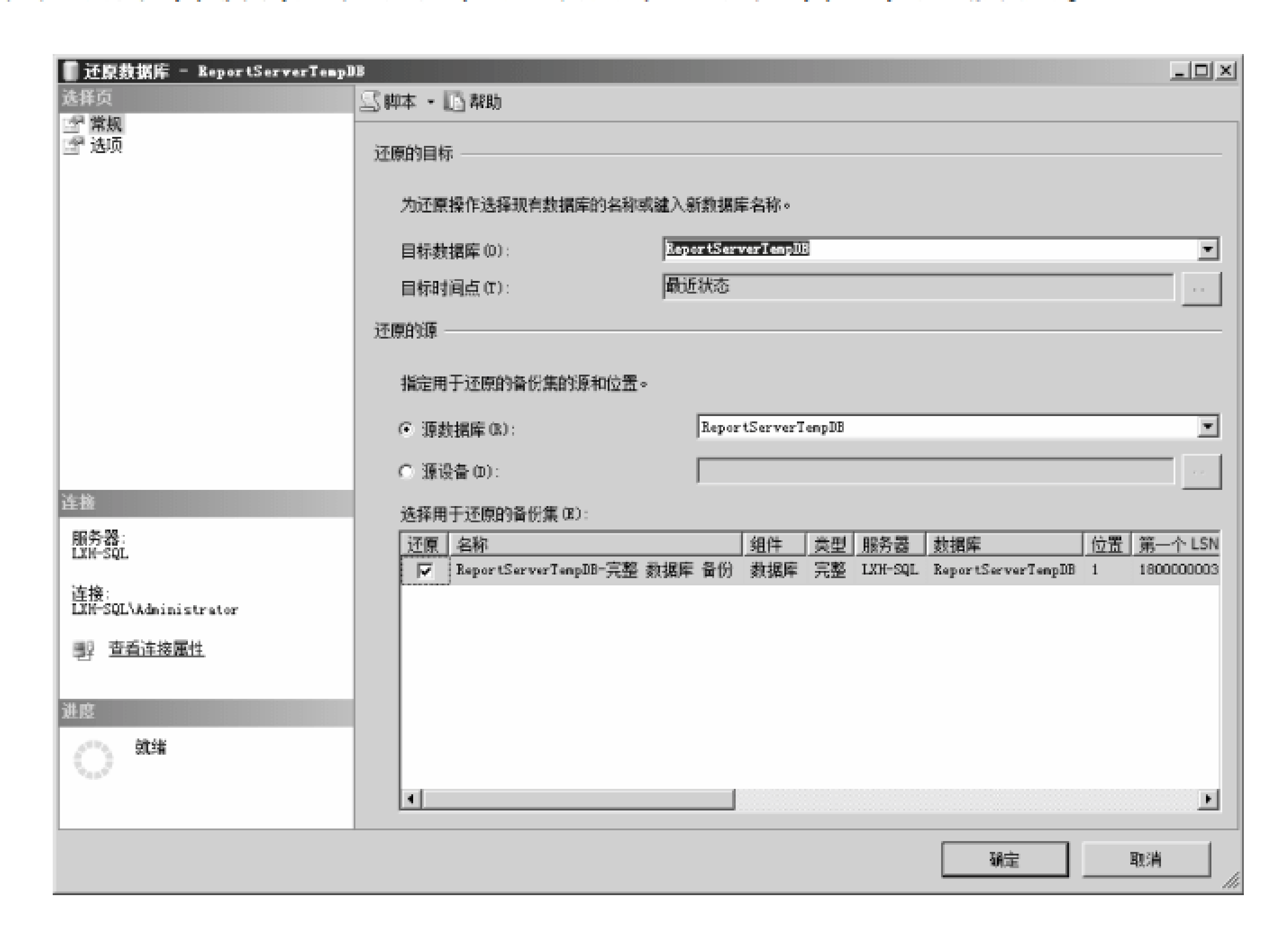


图 13-80　“还原数据库-ReportServerTempDB”对话框

（2）单击“…”按钮，显示“指定备份”对话框。单击“添加”按钮，显示如图 13-81 所示的“定位备份文件”对话框。选择备份的数据库文件，例如“D:\ ReportServerTempDB-081219. bak”。

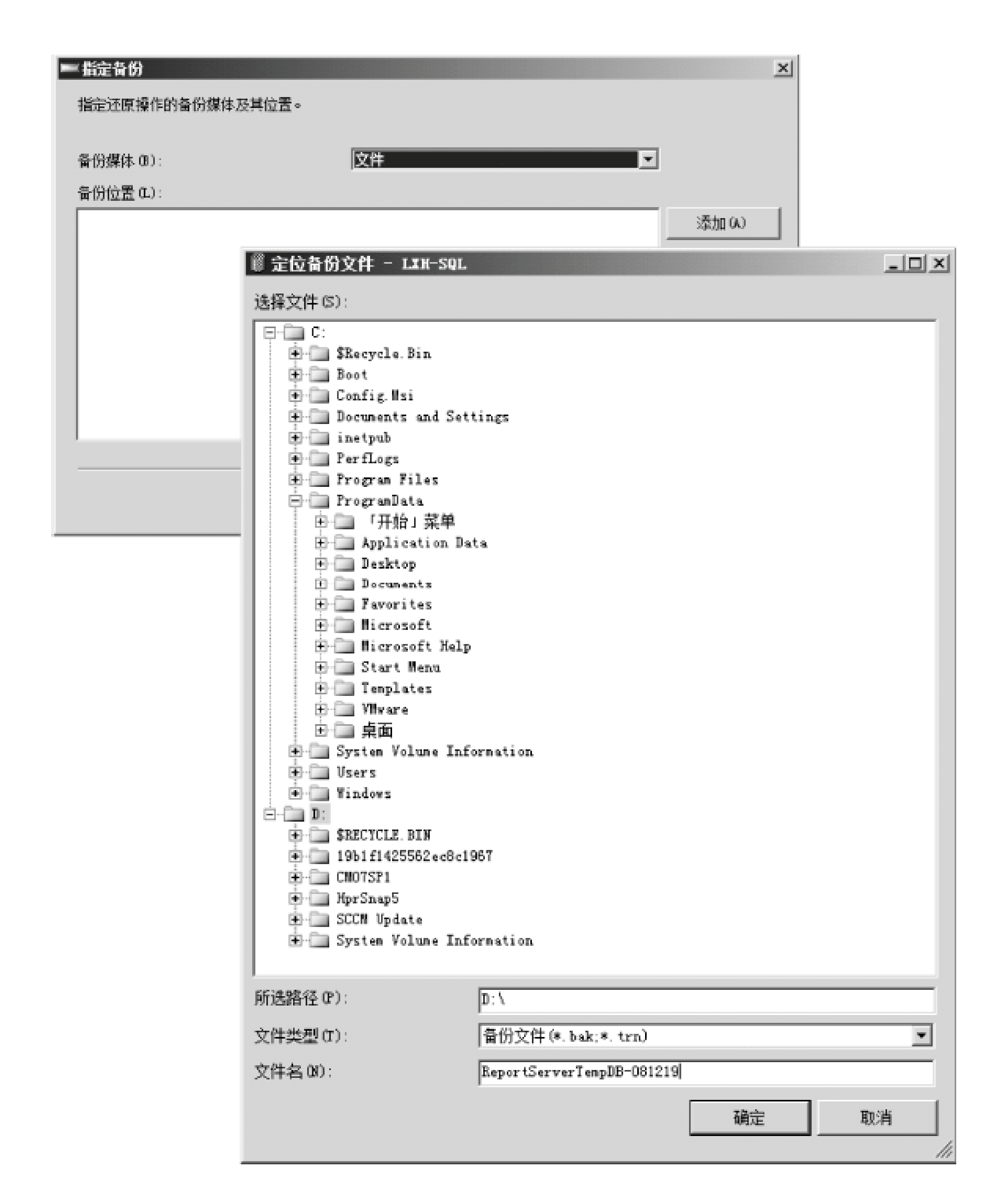


图 13-81　“定位备份文件”对话框

(3) 连续单击"确定"按钮,返回到"还原数据库"窗口,设置完成的还原参数如图 13-82 所示。在"选择用于还原的备份集"分组区域中,选择需要还原的备份文件。

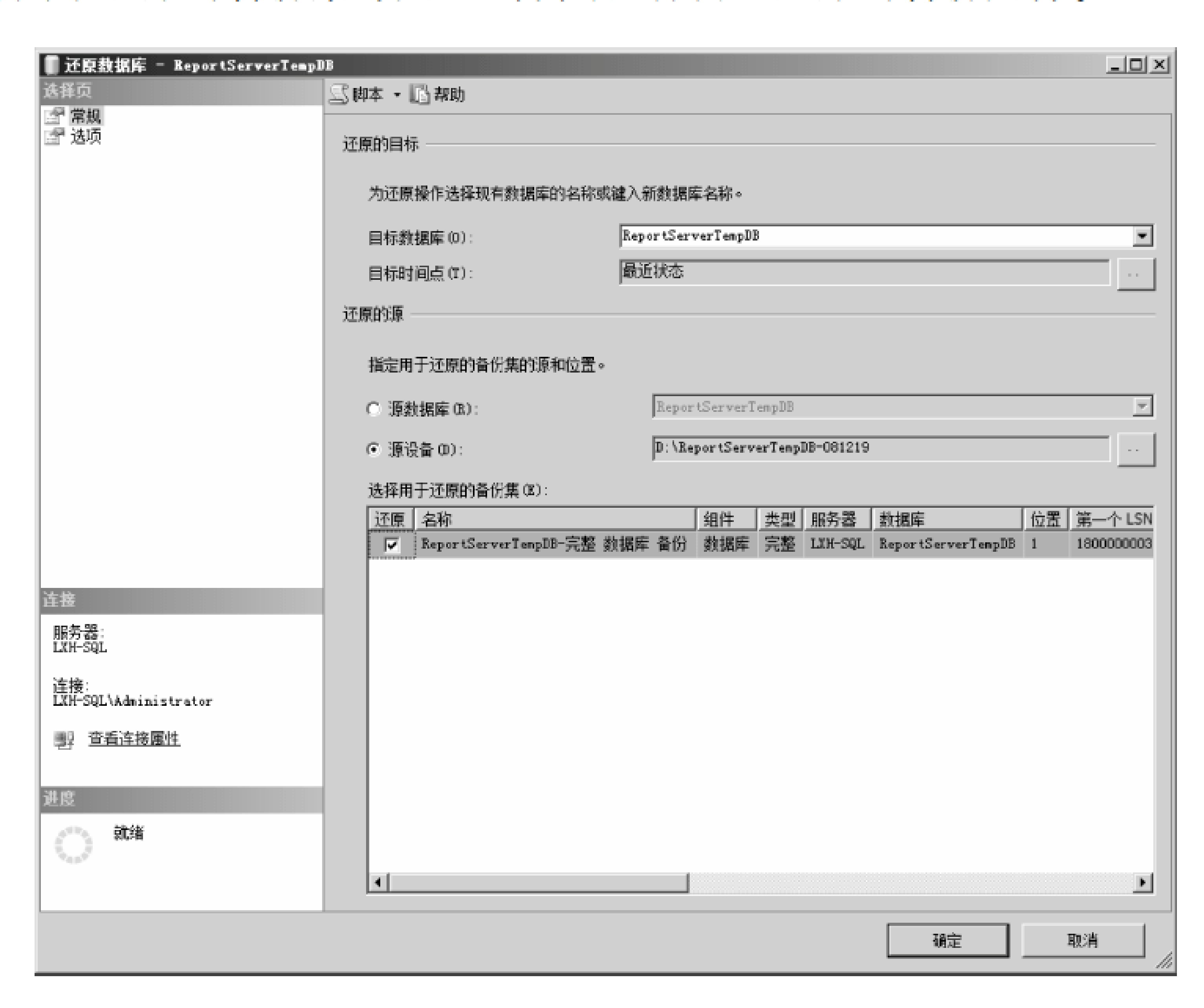


图 13-82 "还原数据库-ReportServerTempDB"对话框

(4) 在"还原数据库"对话框左侧的"选择页"列表中,单击"选项"选项,显示如图 13-83 所示的对话框。

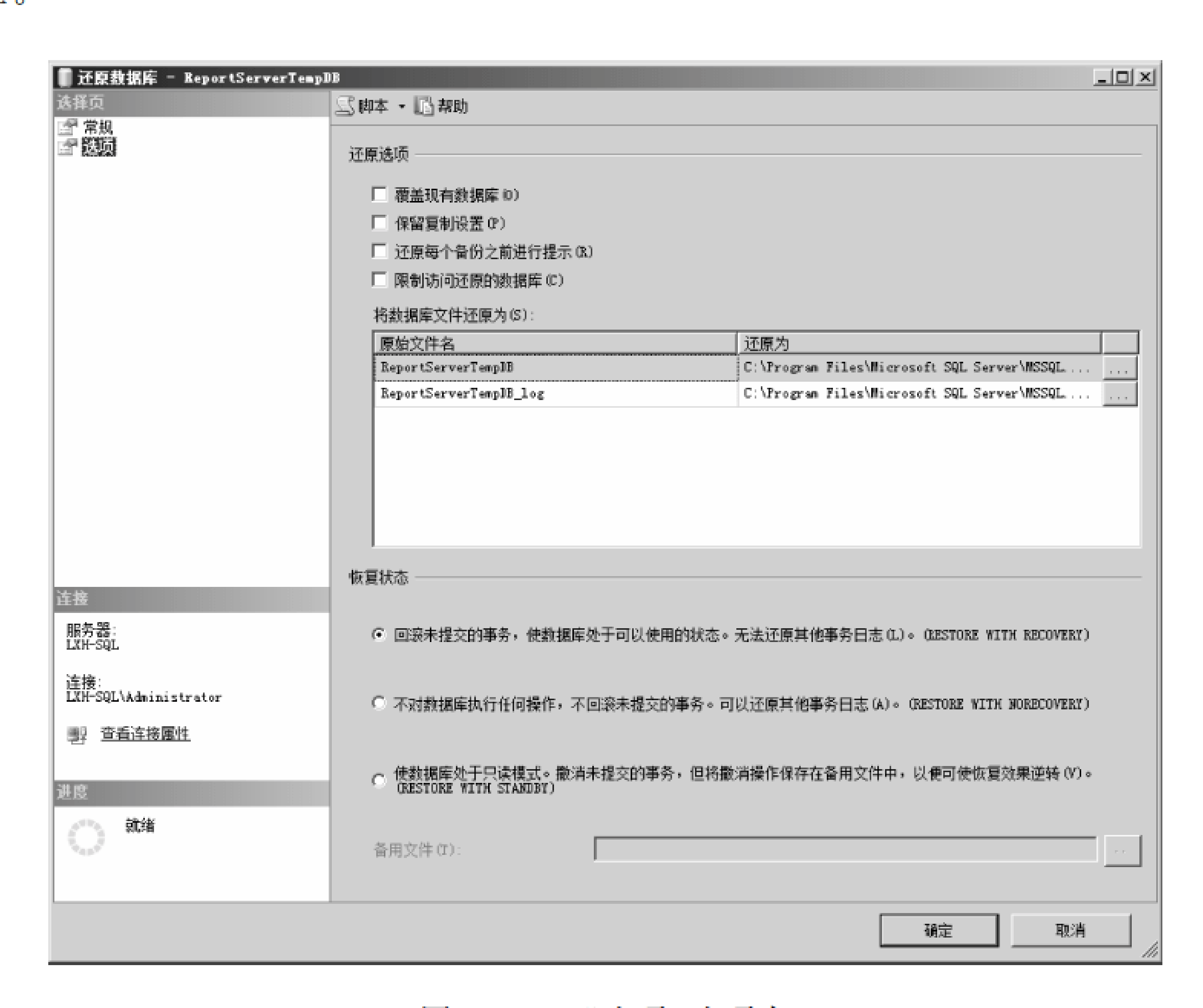


图 13-83 "选项"选项卡

（5）在“还原选项”选项区域中，设置还原的选项。

① 覆盖现有数据库：指定还原操作应覆盖所有现有数据库及其相关文件，无论是否存在同名的其他数据库或文件。

② 保留复制设置：将已发布的数据库还原到创建该数据库的服务器之外的服务器时，保留复制设置。只有在选中“回滚未提交的事务，使数据库处于可以使用的状态”单选按钮时，此选项才可用。

③ 还原每个备份之前进行提示：在还原每个备份设置前要求网络管理员进行确认。

④ 限制访问还原的数据库：还原的数据库仅供 db_owner、dbcreator 或 sysadmin 的成员使用。

（6）在“将数据库文件还原为”选项区域中，指定文件的恢复目标文件夹。默认情况下，显示数据库的原始文件名，网络管理员可以更改要还原到的任意目的文件的路径及名称。

① 原始文件名：源备份文件的完整路径。

② 还原为：要还原的数据库文件完整路径。如果要指定新的还原文件，单击文本框，输入数据库文件路径和文件名。

（7）在“恢复状态”选项区域中，设置数据库的恢复状态。

① 回滚未提交的事务，使数据库处于可以使用的状态。无法还原其他事务日志。RESTORE WITH RECOVERY：恢复数据库。默认选择此项。

② 不对数据库执行任何操作，不回滚未提交的事务。可以还原其他事务日志。RESTORE WITH NORECOVERY：使数据库处于还原状态。若要恢复数据库，使用前面的 RESTORE WITH RECOVERY 选项来执行另一个还原操作。

③ 使数据库处于只读模式。撤销未提交的事务，但将撤销操作保存在备用文件中，以便可使恢复效果逆转。RESTORE WITH STANDBY：使数据库处于备用状态。

（8）单击“确定”按钮，开始执行还原操作，数据库恢复完成显示如图 13-84 所示的 Microsoft SQL Server Management Studio 对话框。



图 13-84　Microsoft SQL Server Management Studio 对话框

习题

1. 简述提高企业网络可靠性的常用方法。
2. 三层交换机端口的 EtherChannel 配置和 Trunking 配置分别实现什么功能？
3. 故障转移群集技术有哪些优点？
4. 简述网络负载均衡技术的功能。
5. 简述群集与网络负载均衡的异同点。
6. 配置路由冗余的两种协议，实现机制有何不同？

实验：配置 WWW 服务器群集

实验目的：

掌握 Windows Server 2008 故障转移群集技术的部署与应用。

实验内容：

部署 Windows Server 2008 故障转移群集服务器，对基于 IIS 的 WWW 服务器进行群集。

实验步骤：

(1) 安装故障转移群集服务角色。

(2) 创建故障转移群集。

(3) 至少准备两台基于 IIS 的 WWW 服务器。

(4) 配置 Web 群集。

(5) 登录客户端并使用群集后的地址访问 Web 站点。

参 考 文 献

1. 刘晓辉,李利军. Windows Server 2008 系统安全管理实战指南[M]. 北京：清华大学出版社,2010
2. 刘晓辉. 网络安全设计、配置与管理大全[M]. 北京：电子工业出版社,2009
3. 刘晓辉,李利军. Windows Server 2008 安全内幕[M]. 北京：清华大学出版社,2009
4. 刘晓辉. 网络安全管理实践(第 2 版)[M]. 北京：电子工业出版社,2009
5. 王春海,王淑江. 网管经验谈[M]. 北京：电子工业出版社,2010
6. 唐任威,赵惊人,张宏义,吕政周. Windows Server 2008 网路服务与安全[M]. 台北：悦知文化,2008
7. Joseph Davies and Tony Northrup with the Microsoft Networking Team(美). Windows Server 2008 Networking and Network Access Protection(NAP)[M]. Redmond Washington：Microsoft Press,2008
8. Jesper M. Johansson and Microsoft MVPs with the Microsoft Security Team(美). Windows Server 2008 Security Resource Kit[M]. Redmond Washington：Microsoft Press,2008